Lucian Blaga University of Sibiu
Faculty of Social Sciences and Humanities
Department of International Relations,
Political Science and Security Studies

STUDIA SECURITATIS JOURNAL

Issued by the
Research Center in Political Sciences, International Relations and European Studies

Two Issues/Year

Editorial board member in charge of the present issue
Nicoleta Annemarie Munteanu, Ph.D.

Volume XVIII
No. 2/2024
ISSN: 2821-5966, ISSN-L: 2821-5966

INTERNATIONAL AFFILIATION

ERIHPLUS
https://dbh.nsd.uib.no/publiseringskanaler/erihplus/

CEEOL
http://www.ceeol.com/

EBSCO
http://www.ebscohost.com/

DOAJ
https://doaj.org/

INDEX COPERNICUS
http://www.indexcopernicus.com/

ULRICH'S PERIODICAL DIRECTORY
http://ulrichsweb.serialssolutions.com/

INFOBASE INDEX
http://www.infobaseindex.com/

SEMANTIC SCHOLAR
https://www.semanticscholar.org/

RESEARCHBIB
http://www.researchbib.com/

MIAR
http://miar.ub.edu

GLOBAL IMPACT & QUALITY FACTOR
http://globalimpactfactor.com/

EDITORIAL BOARD

CO-EDITORS

MEMBERS OF THE INTERNATIONAL SCIENTIFIC BOARD

550324 Sibiu, Calea Dumbrăvii No. 34
Tel. / Fax: +40-269-422169
Web: http://reviste.ulbsibiu.ro/studiasecuritatis/
E-mail: journal.studiasecuritatis@ulbsibiu.ro

CONTENT

ENERGY SECURITY

CIVIL RIGHTS

BOOK REVIEW

Agata KOSIERADZKA-FEDERCZYK
Cardinal Stefan Wyszynski University in Warsaw, Poland

THE LEGAL FRAMEWORK FOR SUPPORTING WAR REFUGEES FROM UKRAINE IN POLAND

Abstract:	*The outbreak of full-scale war in Ukraine resulted in the largest population migration after the Second World War. Poland, as a border country, had to respond to the challenges of the sudden influx of war refugees (around 3 million) within 2 months of the start of the war. It also must respond now, more than two and a half years after the outbreak of war, when there are more than 1 million Ukrainians on Polish territory.* *The article presents the legal solutions introduced in response to the war migration. They concern the following areas: simplification related to legalisation of stay, facilitation of taking up employment and access to social benefits. As there are many children among the migrants, the last area concerns access to school education for Ukrainian children.*
Keywords:	**Migration; law on migration; war on Ukraine; legalislation**
Contact details of the authors:	E-mail: a.federczyk@uksw.edu.pl
Institutional affiliation of the authors:	**Cardinal Stefan Wyszynski University in Warsaw, Poland**
Institutions address:	Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, ul. Dewajtis 5, 01-815 Warszawa, tel. 22 561 88 00, https://uksw.edu.pl/, rektorat@uksw.edu.pl

The Russian aggression against Ukraine has resulted in a humanitarian crisis in the country, with the fastest exodus of refugees in Europe since the Second World War. The scale and pace of the migration have posed and continue to pose a significant challenge to Poland, the country that has received the largest number of refugees. In the 63 days between 24 February and the end of April, a period of just over two months, more than three million people crossed the Polish Ukrainian border[1]. A considerable proportion of war refugees utilized Poland as a transit country, with the majority continuing their journey to other countries, particularly within the European Union, and to a lesser extent, Canada, the USA and Israel. It is estimated that there are currently between 1.2 and 1.5 million Ukrainian refugees in Poland[2].

During the initial stages of the influx, a significant aid campaign was initiated, with millions of Poles offering their assistance on a voluntary basis. The aid provided took a variety of forms, including financial and material assistance, participation in voluntary activities. Surprisingly, despite such a large wave of refugees, not a single refugee camp has been set up in Poland. All those arriving in Poland have found a place in the homes of Poles, or a place organised by various institutions, either NGOs, private individuals, hotels, hostels, etc. According to PIE, the estimated value of Polish private funds committed to assisting refugees in the initial post-war period is PLN 9-10 billion[3]. It was the responsibility of the state to establish suitable structures, including the formulation of an appropriate legal framework for action by public administration bodies, to

[1] Maciej Duszczyk, Paweł Kaczmarczyk, *Wojna i migracja: napływ uchodźców wojennych1 z Ukrainy i możliwe scenariusze na przyszłość*, "CMR Spotlight", Vol. 4 No. 39, 2022, p. 2

[2] *Dwa lata od wybuchu wojny - w Polsce pozostaje ok. 1,5 mln Ukraińców,* https://samorzad.pap.pl/kategoria/aktualnosci/dwa-lata-od-wybuchu-wojny-w-polsce-pozostaje-ok-15-mln-ukraincow (25.10.2024)

[3] Radosław Zyzik, Łukasz Baszczak, Iga Rozbicka, Michał Wielechowski, *Uchodźcy z Ukrainy na polskim rynku pracy: możliwości i przeszkody*, Polski Instytut Ekonomiczny, December 2023, Warsaw, p. 4, https://pie.net.pl/wp-content/uploads/2024/01/Uchodzcy-z-Ukrainy-.pdf (10.10.2024)

facilitate the organization of financial support. The challenge was significant, as Poland had limited experience in accepting refugees and lacked the necessary legal framework to do so effectively. Additionally, Poland has not previously been confronted with such a considerable influx of foreigners who are not proficient in Polish. Furthermore, the last decade has been a period of accelerated transformation for Poland, shifting from a country with a history of emigration to one with a growing immigrant population.

While comparative legal research is attractive, in this article have been kept to a minimum. The purpose of this article was to present the uniqueness of the solutions adopted. They were a state response to an emergency concerning the hosting of war refugees because of a war conflict. It is difficult to assess such legal solutions to those created to shape a planned state policy on migration. While the aim of the latter is to create stable rules of law, in the case of the Ukrainian refugees it is about and quick and adequate response, but also limited in time. It is obvious that current solutions will have to change according to the dynamics of the war conflict. Poland's role as a country bordering the war zone, the scale of migration, the number of refugees remaining in our country, the feeling that state security is threatened, or other such as economic conditions, also limit the possibility to full evaluation and comparison Polish legal solutions with those adopted in other countries. Hence, the aim of this article is to present the extraordinary legal solutions that have been adopted first in Poland. However, the information presented in the article can be used for further research on the legal actions of neighbouring states in relation to waves of war refugees. The objective of this article is to present a select legal solutions taken with the aim of establishing a legal framework that defines the status of war refugees from Ukraine. A primarily dogmatic-legal method was used. Migration data are mainly taken from available online sources of public institutions. This allows the use of up-to-date and reliable data. Due to the vastness of the subject matter, attention has been focused on a few selected areas: legalization of residence, access to the labor market, social benefits and education. Due to the limited framework of the article, even these areas provide a general overview of the situation rather than a detailed analysis.

Migration characteristics

Poland is the country that has received the largest number of refugees from Ukraine, in comparison to all other countries worldwide. Since 24 February 2022, the number of individuals who had crossed the Polish Ukrainian border reached 3.8 million. In February 2024, the number of Ukrainian refugees in Poland ranged from 1.2 to 1.5 million[1]. This figure is based on estimates, as there is no single database that collects comprehensive information. War refugees constitute a distinct migratory group, frequently bearing witness to traumatic events related to armed conflict, which compels them to flee their previous place of residence. This has a detrimental impact on their mental health, social relations and ability to adapt to a new environment, which therefore, has a direct impact on their capacity to function effectively in the professional sphere and distinguishes them from other migrants who may plan their migration in advance[2].

It is notable that the specific demographic profile of refugees from Ukraine to Poland exhibits distinctive characteristics. Approximately 90% of the population are women and children[3]. A recent study conducted by the National Bank of Poland indicates that the largest age group is that of people aged 27-44 (48%), followed by those aged 45-59 (24%) and those under 26 (18%). A total of 9% of refugees are individuals aged 60 or above[4].

From an economic and employment standpoint, it is worth noticing that 61% of refugees possess a university degree. One of the obstacles to accessing work in the learned profession was the challenging process of having a university degree recognized as valid in Poland.

The legal status of the displaced from Ukraine because of the armed conflict - the March 2022 Act

[1] Monitor Deloitte, *Uchodźcy z Ukrainy w Polsce. Wyzwania i potencjał integracji*, October 2022, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Re-ports/pl-Uchodzcy-z-Ukrainy-w-Polsce-Report.pdf (9.10.2024)

[2] Radosław Zyzik, Łukasz Baszczak, Iga Rozbicka, Michał Wielechowski, *Op. cit*., p. 8

[3] https://unicef.pl/co-robimy/aktualnosci/news/okolo-90-uchodzcow -w-polsce-to-kobiety-i-dzieci, (10.10.2024)

[4] National Bank of Poland, *Sytuacja życiowa i ekonomiczna migrantów z Ukrainy w Polsce – wpływ pandemii i wojny na charakter migracji w Polsce. Raport z badania ankietowego*, 2023 https://nbp.pl/wp-content/uploads/ 2024/01/raport_migranci_z-Ukrainy_2023.pdf (10.11.2024)

In Poland, as early as 7 March 2022, a special project of the act was submitted to the Sejm (the parliament) in response to the challenges that arose because of the armed conflict in Ukraine. The act was prepared to resolve vast of urgent problems amongst them the issue of ensuring the legality of the stay of persons coming from the Ukraine. On the same day, the next phase of the legislative process commenced[1].

Subsequently, on 12 March 2022, the Law on Assistance to Citizens of Ukraine in Connection with the Armed Conflict on the Territory of Ukraine (hereinafter referred to as the 'March 2022 Law') was enacted. This legislation represents a distinct departure from the existing legal framework governing migration and asylum, particularly in relation to the following existing laws: The Act of 12 December 2013 on foreigners[2] and the Act of 13 June 2003 on the granting of protection to foreigners on the territory of the Republic of Poland[3]. The regulations in question governed the general rules of migration in times of peace and proved inadequate for the emergency that arose from the war in Ukraine. Polish refugee legislation is the result of the implementation of EU directives on the reception of refugees16 and is largely also based on the content of the Geneva Convention and other international law instruments in force in this matter[4].

The material scope of the March 2022 Act is extremely wide and includes many different types of provisions: legalisation and registration of residence of persons fleeing from Ukraine, forms of support made available to them (in terms of social assistance, education, access to the labour market). In addition, the law regulates the organisation of assistance activities by various public agencies, both governmental and self-governmental, to technical provisions authorising individual institutions to undertake or finance specific activities[5]. Given the circumstances of the Act's adoption, the solutions enshrined within it pertain solely to Ukrainians (or other individuals lacking Ukrainian citizenship) who have arrived in Poland after 24 February 2022. The legislation does not extend to Ukrainian nationals who had previously taken up employment in Poland.

The legislation encompasses three categories of refugees[6]:

1. Citizens of Ukraine and their spouses without Ukrainian citizenship who arrived on Polish territory from Ukrainian territory between 24 February 2022 and the present in connection with military action conducted on its territory;

2. Children born on Polish territory to Ukrainian women who arrived on Polish territory from Ukrainian territory between 24 February 2022 and the present in connection with military action conducted on its territory;

3. Ukrainian citizens holding a Card of the Pole, who departed from Ukraine during the period from 24 February 2022 and then arrived on the territory of Poland with military action conducted on its territory, as well as their immediate family members[7].

As pointed out in the literature, the subjective range of the March 2022 law is broader and goes beyond the narrowly defined 'citizens of Ukraine'[8], which is in line with the specific situation triggered by a war conflict.

---

[1] https://www.sejm.gov.pl/sejm9.nsf/rzebiegProc.xsp?id=9B9CF6ACD09F2BA8C12587FE005B5C89 (10.10.2024)

[2] *Journal of Laws* 2021, Item 2354; hereinafter referred to as: u.c.

[3] *Journal of Laws* 2021, Item 1108 as amended; hereinafter referred to as: u.u.c.o.

[4] Tomasz Szczech, *Integracja uchodźców. Wybrane aspekty prawne*, "Radca Prawny Zeszyty Naukowe", Vol. 3, 2016, p. 99

[5] Witold Antoni Klaus (ed.), *as amended Ustawa o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa*, WKP/el, 2022

[6] From the scope of the regulation were excluded: -holders of a permanent residence permit (art.195 u.c.), a residence permit for a long-term resident of the European Union (art.211 u.c.), a temporary residence permit (art. 98 u.c.), refugee status (art. 13 u.c.c.o.), subsidiary protection (art.15 u.c.c.o.), a permit for tolerated stay (art.351 u.c.), a permit for humanitarian reasons (art. 348 u.c.); -who have submitted applications or declared the intention to submit applications for international protection on the territory of the Republic of Poland, or on behalf of whom such applications have been submitted or the intention to submit an application has been declared (art. 13, art. 15, art. 28 sec. 1, art. 61 sec. 1 u.c.c.o.), unless the application or declaration is withdrawn.

[7] *Law Of 12 March 2022 on Assistance to Citizens Of Ukraine In Connection With Armed Conflict On The Territory Of That Country* Art.2, https://www.gov.pl/web/mswia-en/the-act-on-assistance-to-citizens-of-ukraine-in-connection-with-armed-conflict-on-the-territory-of-that-country-signed-by-the-president (12.11.2024)

[8] Daniel Eryk Lach, *Prawo uchodźców wojennych z Ukrainy do świadczeń opieki zdrowotnej w Polsce*, "Praca i zabezpieczenie społeczne", No. 1, 2023, p. 55

The legalization of residence

The legalization of residence was one of the first issues to be addressed by a special law. This is a prerequisite for subsequent entitlements and benefits, including the ability to seek employment. In adopting a solution to the issue of legal residence, the Polish legislator has chosen to recognize such status as legal by *de jure* if the following conditions are met together:

- Arrival in Poland from 24 February 2022 (or later) in connection with military action conducted on its territory[1];
- Legal entry across the border: it is either in possession of the relevant documents[2] or without. In the latter case, it is required to obtain an entry permit issued by the commanding officer of the Border Guard post[3];
- Declaration of intention to stay in Poland (e.g. commencement of work, submission of application for PESEL number).

To sum up, according to the adopted March 2022 Act, if a citizen of Ukraine has legally arrived on the territory of Poland in the period from 24 February 2022 or later and declares his/her intention to stay on the territory of the Republic of Poland, their status is deemed legal until 30 September 2025[4]. Such simplified conditions allowed for a relatively easy border crossing for those fleeing war territory. Which was additionally important, given that the first and most numerous waves of refugees crossed the border during the winter period. The regulations mentioned above mean that Ukrainians do not have to meet the conditions to enter Poland. The general regulations of migration law in this respect are complex. Firstly, different ones for EU citizens and different ones for citizens from so-called third countries. As Ukraine is not a member of the EU, it does not enjoy the freedom of movement applied to citizens of EU countries.

The general conditions of entry into Poland are very complex and depend on the length of the planned stay and its purpose (e.g. there are differences when the visitor is a student, managerial employee, specialist employee, trainee, researcher, family of a researcher, etc.). In accordance with the general conditions[5], a foreigner crossing the border with the intention to enter the territory of Poland for a time exceeding 90 days is required to provide justification for the purpose and conditions of their planned stay and to possess the following documents: In order to enter Poland, a foreigner must possess the following documents: (1) a valid travel document; (2) a valid long-term visa either residence permit issued by the Polish authorities; (3) a document confirming possession of health insurance; and (4) sufficient financial means to cover the costs of the planned stay and the return journey. Failure to satisfy the conditions may result in the refusal of entry into

[1] Therefore, the scope of the regulation does not cover persons who, although they arrived in Poland after 24.02.2022. - did not leave the territory of Ukraine because of the armed conflict, which in principle may concern a situation where a Ukrainian citizen, prior to 24.02.2022, resided in another country and entered the territory of Poland from that country

[2] E.g. valid travel document, valid visa or other valid document entitling to enter and stay in the territory of the Republic of Poland - Article 23 u.c. and fulfilment of the requirement to justify the reason and conditions of the intended stay, to have financial resources and health insurance cover - Article 25 u.c.

[3] Consent is granted based on the Article 6(5)(c) of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9.03.2016 on the EU Code on the rules governing the movement of persons across borders (OJ EU L 77, p. 1, as amended; hereinafter: Schengen Borders Code). (the possibility to be granted entry on humanitarian grounds, for reasons of state interest or international obligations, despite not meeting entry conditions). Entrance to Poland in violation of the provisions on entry into the Schengen area (Article 5 of the Schengen Borders Code) and crossing the border in violation of the rules with the use of violence, threats, deception or in cooperation with other persons (Article 264 § 2 of the Penal Code) should be regarded as illegal in the context under discussion. Persons who do not meet the commented premise are left with the possibility of seeking international protection on the provisions of the Act on granting protection to foreigners within the territory of the Republic of Poland.

[4] In the March 2022 Act, the end date of the special protection was set at 30 June 2024, but due to the ongoing war, it was extended to 30 September 2025 by the Law of 15 May 2024 amending the Law on Assistance to Citizens of Ukraine in Connection with the Armed Conflict on the Territory of Ukraine and Certain Other Laws (Journal of Laws 2024, item 854)

[5] General regulations are referred to here. It is worth emphasising that the group of refugees is not homogeneous in legal terms, meaning that they are subject to different legal regulations. Read more in the article: Mieczysława Zdanowicz, Zasady legalizacji pobytu cudzoziemców i struktura cudzoziemców w Polsce, "Archiwum Kryminologii", vol. XXXVIII/2016, pp. 441-458

the country. *The March 2022 Act* delineated two grounds for the revocation of the right to remain in Poland for Ukrainian citizens. The first of these grounds pertains to leaving Poland for a time exceeding 30 days, which is understood an intention to abandon the original plan to remain in Poland. The second ground for depriving a Ukrainian citizen of the right to stay in Poland is the use by such a citizen of temporary protection on the territory of another European Union member state, granted due to military operations conducted on the territory of Ukraine[1]. Obtaining a PESEL number and registration as a refugeeing in the state systems entitles Ukrainians to freely utilize public services, including the receipt of certain benefits or the registration of their own business. It is possible to obtain a trusted profile, which enables the completion of official transactions via the Internet.

Access to the labor market

The March 2022 Act introduced several measures designed to facilitate access to the labor market. In this respect, too, it is indicated that it has a significant impact on the shape of the national labor market[2]. In accordance with the legislation, Ukrainian nationals who are legally resident in Poland are entitled to utilize the labor market services available to Polish citizens. The most significant entitlement is the capacity to pursue legal employment with any employer in Poland, without the necessity of fulfill additional formalities. Furthermore, they are entitled to benefit from job placement, vocational guidance and training. A specific procedure has been established for registering with the labor office as either unemployed or a jobseeker. This is conducted in accordance with the same regulations as for Polish citizens, with the exception that no PESEL is required for registration at the labor office. Instead, a passport or identity card, or a certificate from the Border Guard or a municipal office is sufficient. Ukrainian citizens are entitled to set up sole proprietorship on an equal footing with Polish citizens. The only prerequisite is the acquisition of a PESEL number. A jobseeker may contact the district employment office, utilize the ePraca mobile application, or contact the relevant authority via a dedicated hotline. Furthermore, a new section of the portal has been created for Ukrainian citizens.

To sum up – the polish legislature has eliminated the requirement for a work permit for Ukrainian nationals as a prerequisite for employment. The *onus* is on the employer to notify the labor office of the employment of the Ukrainian citizen within 14 days of the commencement of employment. This is the sole formal condition. This constitutes a significant simplification considering the general regulations set forth in the Law on Foreigners, which stipulate that a foreigner must possess a valid visa or temporary residence permit to work in Poland.

A review of public registers and relevant research findings suggests that refugees are highly active in the labor market. Although Ukrainian refugees are integrating into the labor markets of their host countries at a significantly faster pace than other refugee groups, compared to OECD countries, it is in our country that the employment rate of war refugees is the highest at 65%. This is particularly significant given that the primary motivation for refugees to come to our country was not financial, but rather the desire to distance themselves and their families from the threat to their lives[3]. The prior involvement of Ukrainian nationals in the Polish labor market has constituted a facilitating factor in the integration of refugees into the Polish labor market. The available data indicates that in 2021 alone, 325,000 documents authorizing long-term employment were issued for this nationality[4]. Conversely, the total number of Ukrainians employed in Poland at that time was estimated to be 1.5 million[5].

---

[1] *March 2022 Act, art. 11*

[2] Krzysztof Jurek, *Polski rynek pracy dla uchodźców z Ukrainy*, "Kultura Bezpieczeństwa", Vol. 42, 2022, p.13

[3] Radosław Zyzik, Łukasz Baszczak, Iga Rozbicka, Michał Wielechowski, *Uchodźcy z Ukrainy na polskim rynku pracy: możliwości i przeszkody*, Polski Instytut Ekonomiczny, December 2023, Warsaw, p. 4-6. In Poland, the percentage of employed Ukrainians is significantly higher compared to other neighbours - in Lithuania it is 53 %, in the Czech Republic 51 %, in Slovakia 34 % and in Germany 18 %). This result can be considered a considerable achievement, given that Ukrainian refugees active on the Polish labour market represent a wide spectrum of qualifications and work experience, making their professional integration a complex and diverse process.

[4] Ministry of Labour and Social Policy, https://www.bankier.pl/wiadomosc/2021-r-rekordowy-pod-wzgledem-liczby-cudzoziemcow-na-polskim-rynku-pracy-8271907.html (10.10.2024)

[5] Zyzik, Baszczak, Rozbicka, Wielechowski, *Op. cit.*, p. 8

The first quarter of 2022 saw the highest number of vacancies in the Polish economy, with 159,000 vacancies recorded. It appears that there was considerable scope for the integration of refugees into the Polish labor market, and the Polish economy should be well placed to accommodate a significant proportion of the working-age arrivals. It is, however, important to note that most vacancies were concentrated in sectors such as transport, construction and warehouse management, which do not align with the profile of migrants. Up until that date, the gap had been partially addressed by the influx of male migrants from Ukraine. The war caused them to return home, resulting in an exodus of workers previously employed, which consequently added to the already large number of vacancies in these sectors. In 2022, Poland witnessed a notable reduction in the inflow of temporary workers, with a 26% decline compared to the previous year[1].

Access to social benefits

The March 2022 Act introduced specific provisions regarding access to social benefits. The legislation grants the right to various types of benefits. The entitlement to benefits is contingent upon and extends throughout the period of legal residence in Poland, applying to both parents and children. Parents (or guardians) applying for benefits are exempt from the obligation to hold a residence card with the annotation 'access to the labor market. Ukrainian refugees were granted a one-off cash benefit of PLN 300 (70 Euro) per person for subsistence, with the objective of covering essentials such as food, clothing, footwear, personal hygiene products and accommodation costs.

Additionally, they were provided with access to family benefits. The family allowance is designed to offset a portion of the costs associated with raising a child. The entitlement to the allowance is contingent upon several factors, including the per capita family income not exceeding the specified threshold of PLN 674 (155 Euro) or PLN 764 (176 Euro) in cases where a disability child lives in the family. Other family allowances are linked to specific circumstances, including the birth of a child (as a one-off payment), the care of a child during parental leave (as a monthly payment), and single parenthood. *The March 2022 Act* introduced access to special care benefits, including a nursing allowance to cover the costs of providing care and assistance to another person due to their inability to live independently, and a nursing benefit for those who have resigned from employment. The benefit is granted when individuals refrain from pursuing or relinquishing gainful employment to provide care for another individual.

The upbringing benefit, commonly referred to as 800+, is designed to partially cover the costs associated with raising a child, including their care and meeting their basic living needs (500 PLN – 115 Euro until the end of 2023, now 800 PLN – 184 Euro). The allowance is paid monthly and is set at a fixed amount of PLN 800 (184 Euro) per child up to the age of 18. The benefit is granted irrespective of the family's income[2]. Independently of the support for Ukrainians, Poland has also offered financial support to Polish families who have welcomed Ukrainian refugees. This has included a financial allowance of 40 PLN (9 Euro) per day for the accommodation of a Ukrainian citizen.

Access to education for Ukrainian children

Another area that required immediate attention was the participation of Ukrainian children in the education system. It should be noted that Ukrainian pupils were the largest group of foreign children in Poland even before the Russian full-scale aggression against Ukraine. However, the children of economic migrants predominated among them, whereas after 24th of February 2022 we are dealing with a massive influx of pupils with refugee experience, whose situation is markedly different from that of their classmates who arrived here earlier[3]. Inclusion of newly arrived pupils was an aspect of significant importance for several reasons. Firstly, the structure of migration meant that, in the initial phase of the migration wave, a considerable proportion of migrants were mothers with children. It is estimated that in the initial three-month period of the war, over three million individuals from Ukraine arrived in Poland, with 43% of this number comprising children and

[1] OECD, p. 26

[2] *March 2022 Act, art. 26*

[3] Katarzyna Stankiewicz, Anna Żurek, *Edukacja dzieci uchodźczych w Polsce*, "Infos. Zagadnienia Społeczno-Gospodarcze", Biuro Analiz Sejmowych, Vol. 5, 2022, p. 1

adolescents up to the age of 17[1]. The right to education is one of the fundamental human rights, guaranteed and regulated by many international conventions and agreements. The education system plays a very important role in the process of counteracting the social exclusion and integration of Ukrainian refugees into Polish society[2]. Moreover, ensuring access to pre-school and school care was a prerequisite for adult migrants to commence employment.

In this regard, legal solutions can be divided into two periods. In the initial phase, the Polish state facilitated access to its educational institutions for Ukrainian children and young people. The decision of whether a Ukrainian parent would avail themselves of this option was at their discretion. It was possible for children to pursue their classes within the Ukrainian system, either remotely or in a mixed mode. This resulted in some children remaining outside the Polish educational system. This meant that the Polish state had no information as to whether such children were fulfilling any educational obligation. This presented a significant risk to the proper development of children. Non-governmental organizations, including Ukrainian ones, have advocated for amendments to the legislation that would require the thousands of Ukrainian children and young people residing in Poland to attend school. They have estimated that there could be between 100,000 and 200,000 Ukrainian children aged 3 to 18 who are currently outside the educational system[3].

Remaining in education provides a secure environment for the child. The educational establishment represents a setting in which individuals can not only gain knowledge and prepare for future careers, but also develop social competencies through the formation of relationships and the acquisition of knowledge about the needs and problems of their peers. These arguments, among others, have led to the conclusion that, as of 1 September 2024, refugee children from Ukraine will be included in the Polish educational system. This will entail their participation in compulsory annual pre-school preparation, compulsory schooling and compulsory education (post-primary schools), on an equal footing with Polish pupils. In the 2024/2025 academic year, online learning has been permitted solely for pupils enrolled in the highest program class within a Ukrainian education system school. It is possible for them to complete their education via the online format. To encourage attendance at Polish schools, Ukrainian pupils are exempt from taking the Polish language exam at the eighth grade (Polish 8th grade) examination. Furthermore, the period of supplementary free Polish language tuition for refugee pupils has been extended from 24 to 36 months[4], and an intercultural assistant has been introduced.

As of September 2024, the completion of compulsory education has been linked to the entitlement to receive a portion of social benefits. Refugees from Ukraine who receiving the Family Benefit 800+ and Good Start will be eligible for payment on the condition that their child is enrolled in pre-school, primary school or secondary school. While the decision to provide compulsory education for the children of Ukrainian refugees is a positive one, it is important to recognize that this is, and will continue to be, a challenging undertaking for schools from an organizational perspective. The available research indicates that Ukrainian students tend to perform well in Polish schools[5]. However, Polish schools were unprepared to accommodate such many foreign language students in their classrooms. As a result, Ukrainian students were placed in classes that were already at or near maximum capacity, with Polish pupils. From the outset, pupils were required to participate in lessons conducted in Polish, which presented a significant challenge for the pupils themselves, their parents and the teachers, who lacked the requisite language skills to communicate effectively with them. A deficiency

[1] Gov.pl., *Uczniowie z Ukrainy w polskich szkołach. Ważne informacje dla rodziców / Учні з України в польських школах. Важлива інформація для батьків*, https://www.gov.pl/web/edukacja/uczniowie-z-ukrainy-w-polskich-szkolach-wazne-informacje-dla-rodzicow, (18.10.2024)

[2] Krzysztof Piotr Jurek, Iwona Niewiadomska, Alina Betlej, *Proces integracji społecznej dzieci ukraińskich w polskim systemie oświaty*, Wydawnictwo Adam Marszałek, Toruń 2022, p. 13

[3] Izabela Kacprzak, *Szkoły muszą zmieścić 80 tys. dzieci z Ukrainy*, https://www.rp.pl/edukacja/art40868721-szkoly-musza-zmiescic-80-tys-dzieci-z-ukrainy (18.10.2024)

[4] Jędrzej Witkowski and Elżbieta Świdrowska shows that 40% of Ukrainian pupils do not benefit from additional Polish language lesson, Uczniowie z Ukrainy, *Co mówią nowe dane? Komentarz*, Centrum Edukacji Obywatelskiej, https://ceo.org.pl/co-wiemy-o-uczniach-z-ukrainy-z-doswiadczeniem-uchodzstwa-w-polskiej-szkole/, (18.10.2024)

[5] Magdalena Tędziagolska, Bartłomiej Walczak, Kamil M. Wielecki, *Uczniowiei uczennice z Ukrainy wpolskich szkołach -rok szkolny 2023/2024 Raport z badań jakościowycj*, p. 4, https://ceo.org.pl/wp-content/uploads/2024/10/Ukrainscy-uczniowie-w-polskiej-szkole_raport-CEO_UNICEF_PL.pdf (18.10.2024)

of psychological support for those suffering from war trauma persists[1]. This is merely a sampling of the challenges confronting Polish educational institutions. There are numerous additional issues.

Conclusions

In conclusion, while the measures taken by the Polish state in response to the influx of Ukrainian refugees have not always been entirely effective, the prompt implementation of a dedicated legislative framework has yielded significant benefits. First and foremost, the expeditious enactment of the special law, which delineated the legal status of refugees and facilitated their swift integration into the Polish social system and labor market, proved instrumental in this regard. This prevented any adverse consequences for the Polish state. As a result, the adverse consequences that would have arisen from the delay in refugees' access to the labor market, which would have resulted in significant losses and lower employment rates, were averted[2].

As a result of the swift and decisive action taken by Poland, the potential for a significant negative impact on the labor market was averted. This was particularly evident in the case of refugees arriving in Europe during the 2015-16 period[3]. The success of refugee integration in the long term is contingent upon the provision of requisite support in the initial weeks and months of their stay in Poland. This is essential for ensuring stabilization and professional development for adults and education and training for youth and children. The immediate measures taken have undoubtedly produced many positive results. The time for an emergency response is already long gone, and the organization of the stay of Ukrainian refugees needs systemic and sustainable solutions.

Bibliography

Books

1. Klaus, Witold, Antoni (Ed.), *Ustawa o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa*, WKP/el, 2022
2. Jurek, Krzysztof, Piotr; Niewiadomska, Iwona; Betlej, Alina, *Proces integracji społecznej dzieci ukraińskich w polskim systemie oświaty*, Wydawnictwo Adam Marszałek, Toruń, 2022

Studies and Articles

1. Duszczyk, Maciej; Kaczmarczyk, Paweł, *Wojna i migracja: napływ uchodźców wojennych1 z Ukrainy i możliwe scenariusze na przyszłość*, „CMR Spotlight", Vol. 39, No. 4, April, 2022
2. Jurek, Krzysztof, *Polski rynek pracy dla uchodźców z Ukrainy*, "Kultura Bezpieczeństwa", Vol. 42, 2022
3. Lach, Daniel, Eryk, *Prawo uchodźców wojennych z Ukrainy do świadczeń opieki zdrowotnej w Polsce*, "Praca i zabezpieczenie społeczne", No. 1, 2023
4. Stankiewicz, Katarzyna; Żurek, Anna, E*dukacja dzieci uchodźczych w Polsce*, "Infos. Zagadnienia Społeczno-Gospodarcze", Biuro Analiz Sejmowych, Vol. 5, 2022
5. Szczech, Tomasz, *Integracja uchodźców. Wybrane aspekty prawne*, "Radca Prawny Zeszyty Naukowe", Vol. 3, 2016
6. Tędziagolska, Magdalena; Walczak, Bartłomiej; Wielecki, Kamil, M., *Uczniowie i uczennice z Ukrainy w polskiej szkole – rok szkolny 2023/24*" https://ceo.org.pl/wp-content/uploads/2024/10/Ukrainscy-uczniowie-w-polskiej-szkole_raport-CEO_UNICEF_PL.pdf
7. Witkowski, Jędrzej; Świdrowska, Elżbieta, *Uczniowie z Ukrainy. Co mówią nowe dane? Komentarz, Centrum Edukacji Obywatelskiej*, https://ceo.org.pl/co-wiemy-o-uczniach-z-ukrainy-z-doswiadczeniem-uchodzstwa-w-polskiej-szkole/
8. Zdanowicz, Mieczysława, *Zasady legalizacji pobytu cudzoziemców i struktura cudzoziemców w Polsce*, "Archiwum Kryminologii", vol. XXXVIII, 2016

[1] *Ibidem*, p. 8 et seq

[2] The early opening of the labour market in Poland avoided the serious consequences that resulted from the exclusion from the labour market of refugees arriving in Europe in 2015-16 - €4,000 loss per refugee per year; - 24 % lower probability of employment in the first 2-4 years after migration; - 9 % lower labour force participation 8 years after arrival.

[3] Monitor Delloite, *Op. cit*., p. 15

9. Zyzik, Radosław; Baszczak, Łukasz; Rozbicka, Iga; Wielechowski, Michał, *Uchodźcy z Ukrainy na polskim rynku pracy: możliwości i przeszkody*, Polski Instytut Ekonomiczny, December 2023, Warsaw, https://pie.net.pl/wp-content/uploads/2024/01/Uchodzcy-z-Ukrainy-.pdf

Documents

1. Monitor Deloitte, *Uchodźcy z Ukrainy w Polsce. Wyzwania i potencjał integracji,* October, 2022, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Re-ports/pl-Uchodzcy-z-Ukrainy-w-Polsce-Report.pdf
2. National Bank of Poland, *Sytuacja życiowa i ekonomiczna migrantów z Ukrainy w Polsce – wpływ pandemii i wojny na charakter migracji w Polsce. Raport z badania ankietowego*, 2023 https://nbp.pl/wp-content/uploads/ 2024/01/raport_migranci_z-Ukrainy_2023.pdf

Websites

1. https://samorzad.pap.pl
2. https://unicef.pl/
3. https://www.bankier.pl/
4. https://www.gov.pl/
5. https://www.rp.pl/
6. https://www.sejm.gov.pl/

Eugen STRĂUȚIU (1)
Lucian Blaga University of Sibiu, Romania
Cristina-Alexandra DEFFERT (2)
Lucian Blaga University of Sibiu, Romania

DIVIDED CITIES: A CASE STUDY ON RECENT EVENTS IN MITROVICA

Abstract:	*The city of Mitrovica, located in the north of Kosovo province, went through a bloody phase during the war in 1999, when almost the entire Roma population was evacuated from the town and the Serb population, originally living on the south bank of the Ibar River, was resettled on the north bank.* *Today, Mitrovica remains an ethnically and religiously segregated town, the object of peace-keeping missions by KFOR (Kosovo Force) and the United Nations Interim Administration Mission in Kosovo (UNMIK). Violent clashes between nationalities, or between the Serb population and the authorities, have recurred several times.* *The objective recapitulation of events is the first step towards a correct understanding of the phenomenon and then to sketch out scenarios of pacification and civilized coexistence of nationalities. Our research aims to provide an updated listing of the main moments in the recent history of the conflict, based on which we will contribute to a correct understanding and prioritization of the causes, detail and explain the current picture of the problem, and then sketch some scenarios for solutions. We will add a brief comparative look, with explanatory value, on other cases of divided cities, to grasp the common and different elements.* *To this end, we will use tools specific to history, political science, cultural studies and security studies. We will operate with document analysis, causal analysis, comparative analysis and case study, in the hope of getting as close as possible to the correct explanations and feasible solutions.*
Keywords:	**Kosovo War; Mitrovica; divided city; ethnic conflict; separatism**
Contact details of the authors:	E-mail: eugen.strautiu@ulbsibiu.ro (1) cristinaalexandra.deffert@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Department of International Relations, Political Science and Security Studies, Lucian Blaga University of Sibiu, Romania (1) (2)**
Institutions address:	Calea Dumbrăvii No. 34, 2nd Floor, 550324, Sibiu, Romania, phone 0040269422169 (1) (2)

Introduction

The problem of divided cities has benefited from the attention of international researchers, who have offered less theoretical approaches (with rather superficial approaches in terms of definitions, characterizations, classifications), and more case studies. In Romania, this topic does not seem to have been interesting at all. The main explanation lies in the lack of cases of towns divided along ethnic and/or cultural lines throughout the country. In the Romanian case, absolute segregation was characteristic of Transylvanian cities until the mid-19th century (the interior of the cities being reserved, by drastic legislation, for constitutionally "recognized nations" - from which Romanians were excluded)[1]. In the two extra-Carpathian "voivodates", we have witnessed a numerical, economic

[1] Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow, *Unio Trium Nationum*, Betascript Publishing, Beau Bassin, 2011

and cultural domination of the urban landscape by ethno-religious minorities, with Romanians representing insignificant minorities[1].

Based on this reality, during the Austro-Hungarian dualism (1867-1918) and especially during the Communism (1945-1989), the cities experienced a constant infusion of Romanian population, in a generally peaceful and constructive multicultural atmosphere, so that the segregation of cities along ethnic lines was not perpetuated.

At the same time, in the immediate vicinity of Romania, divided cities are both a historical and (especially) a contemporary reality. The cases of Mostar (Bosnia-Herzegovina)[2] and Mitrovica (Kosovo) are the best known, with Mostar being researched more often and in greater depth. Due to the nature of the problem, the methodological approach of our thematic approach implies multi-disciplinarity, with history, cultural studies, economics, law, political science, security studies - and not only - contributing to the presentation and explanation of the phenomenon.

In the present research, we aim to provide a brief theoretical framework of the problem of segregated cities, as a context for further elaboration of the case of Mitrovica in Kosovo - where we will emphasize especially the recent state of the phenomenon, which is little studied by scholars. Among the works that place the Mitrovica problem in the paradigm of divided cities, we mention the article by Anna Jarstad and Sandra Segall, *Grasping the Empirical Realities of Peace in Post-war Northern Mitrovica* (2019)[3] and the volume chapter of Pinos Jaume Castan *Mitrovica: A City (Re)Shaped by Divisions* (2016)[4].

Divided cities. Some theoretical approaches

The topic of divided cities began to be systematically explored in the context of the civil war in the former Yugoslavia in the early 1990s. Peter Marcuse's landmark study, *What's So New About Divided Cities?* published in the "International Journal of Urban and Regional Research"[5]. Among the definitions circulated in the research literature, we note that of Rabinowitz and Monterescu, in 2008: divided cities are characterized by "barriers of race, religion, and nationality, encoded in dualistic metaphors of East and West, uptown and downtown, and northside and southside"[6]. In contrast, mixed cities present themselves as "a certain mix in housing zones, ongoing neighborly relations, socioeconomic proximity, and various modes of joint solidarity", in which "individuals and groups on both sides actually share elements of identity, symbolic traits, and cultural markers, signifying the mixed town as a locus of joint memory, affiliation, and self-identification"[7]. Joel Kotek refers to the same phenomenon of segregated cities as the "border city", which he defines as follows: "that are not only polarized on an ethnic or ideological basis (cf. Berlin during the Cold War), but are, above all, disputed because of their location on fault-lines between ethnic, religious or ideological wholes"[8]. Other reference works, such as the OECD's 2018 report *Divided Cities: Understanding Intra-Urban Inequalities*, lists several causes and criteria for city segregation, including income (the gap between rich and poor), the presence of migrants (the extent to which they form separate communities), the accessibility of transportation (both public and personal)[9]. In a more elaborate form, the factors of urban segregation can be classified into two broad categories: cultural and socio-economic. In the first category is religion, then identity/ethnicity/nationality, and finally culture/language. In the second category, we talk about

[1] Laurențiu Rădvan, *Orașele din țările române în evul mediu (sfârșitul sec. al XIII-lea – începutul sec. al XVI-lea)*, Editura Universității „Alexandru Ioan Cuza", Iași, 2011, pp. 215-222

[2] Giulia Carabelli, *The Divided City and the Grassroots. The (Un)making of Ethnic Divisions in Mostar*, Palgrave MacMilan, Singapore, 2018

[3] Anna Jarstad, Sandra Segall, *Grasping the Empirical Realities of Peace in Post-war Northern Mitrovica*, "Third World Thematics: A TWQ Journal", Vol. 4, No. 2-3, 2019, pp. 239-259

[4] Jaume Castan Pinos, *Mitrovica: A City (Re)Shaped by Divisions*, in É. Ó Ciardha, G. Vojvoda (Eds.), *Politics of Identity in Post-conflict States*, Routledge, London, 2016, pp. 128–142

[5] Peter Marcuse, *What's So New About Divided Cities?*, "International Journal of Urban and Regional Research", Vol. 17, Issue 3, 1993, pp. 355-365

[6] D. Rabinowitz, D. Monterescu, *Reconfiguring the "Mixed Town": Urban Transformations of Ethnonational Relations in Palestine and Israel*, "International Journal of Middle East Studies", Vol. 40, 2008, p. 217

[7] *Ibidem*, p. 198

[8] Joel Kotek, *Divided Cities in the European Cultural Context*, "Progress in Planning", No. 52, 1999, p. 228

[9] OECD, *Divided Cities: Understanding Intra-urban Inequalities*, OECD Publishing, Paris, 2018

competition for economic resources and demographic change[1]. Several more recent case studies, in a non-exhaustive presentation, propose comparative analysis (Belfast, Beirut, Jerusalem, Mostar, and Nicosia)[2] or focused analysis, with reference to Beirut as neighborhood planning [3], Sao Paolo as a city of organized crime[4], Berlin as a geopolitically divided city[5], Jerusalem as a divided Holy City[6] etc.

Overview of Mitrovica: historical context, urban space and division

Mitrovica, a city in northern Kosovo, situated at a strategic crossroads in the Balkans, has a tremendously complex historical background, shaped by various political entities. The earliest references to Mitrovica date back to the Ottoman period, when it emerged as a modest Turkish-Eastern settlement; however, its urban development was significantly influenced by its geographic context and the dynamics of neighboring settlements, particularly Trepča and Zvečan[7]. As Zvečan's military significance waned and Trepča's mining operations declined, Mitrovica began to flourish, ultimately achieving recognition as a "varoš"[8] (city) by the late 19th century, following the construction of the railway in 1873[9]. Thus, the interplay of favorable geographical conditions, agricultural resources, and its position as a communication junction facilitated its transition from a relatively insignificant settlement to a prominent urban center in the region.

Furthermore, Mitrovica has historically exemplified a multicultural environment. Kosovo has always been a pluralistic society in which diverse ethnic groups have coexisted, communicating in several languages and practicing the main Balkan religions (Orthodox Christianity, Islam, Judaism), with urban centers serving as pivotal places for this cultural plurality[10]. This phenomenon was and remains very evident in Mitrovica, where significant demographic changes took place with the construction of the railway as it not only facilitated the influx of diverse populations, including merchants, craftsmen and workers from different backgrounds, but also catalyzed the growth of the city as a commercial and administrative center[11]. In addition, the complex social fabric of Mitrovica can be understood within the context of the Ottoman "millet" system[12], which structured the identities and rights of various religious and ethnic communities. The distinction between Muslims and non-Muslims underpinned the Ottoman social hierarchy, yet religious affiliation was not the sole marker of identity; administrative classifications and local contexts shaped community interactions[13]. Consequently, Mitrovica emerged as a cultural microcosm, where the interplay of diverse groups contributed to its urban development and economic vitality.

---

[1] Gizem Caner, Fulin Bölen, *"Multicultural" Cities or "Divided" Cities: What Makes the Difference?*, Conference Paper, 2012 p. 3, https://www.researchgate.net/publication/272833411_%27Multicultural%27_cities_or_%27divided%27_cities_what_makes_the_difference?enrichId=rgreq-ecbc96bd33f3fef7d17beefed907b8b7-XXX&enrichSource=Y292ZXJQYWdlOzI3MjgzMzQxMTtBUzo2NTUxMjY3NzE1NTYzNTNAMTUzMzIwNTgwMjY5MA%3D%3D&el=1_x_2&_esc=publicationCoverPdf (10.10.2024)

[2] Jon Calame, Esther Charlesworth, Lebbeus Woods, *Divided Cities: Belfast, Beirut, Jerusalem, Mostar, and Nicosia*, University of Pennsylvania Press, 2009

[3] David Aouad, *Neighborhood Planning for a Divided City: The Case of Beirut*, "Urban Planning", Volume 7, Issue 1, 2022, pp. 129–141

[4] Teresa P. R. Caldeira, *City of Walls: Crime, Segregation, and Citizenship in São Paulo*, University of California Press, Berkeley, 2000

[5] Hartmut Häußermann, Andreas Kapphan, *Berlin: From Divided to Fragmented City?. Socio-Spatial Changes Since 1990*, in Hartmut Häußermann, Andreas Kapphan (Eds.*) Berlin: von der geteilten zur gespaltenen Stadt? Sozialräumlicher Wandel seit 1990*, Leske + Budrich, Opladen, 2013, pp. 77-94

[6] Bernard Wasserstein, *Divided Jerusalem: The Struggle for the Holy City*, Yale University Press, Yale, 2008

[7] Jaume Castan Pinos, *Mitrovica: A City (Re)Shaped by Division*, "Politics of Identity", Vol. 29, No. 9, 2015, pp. 128-142.

[8] Vjeran Kursar, *Being an Ottoman Vlach: On Vlach Identity (Ies), Role and Status in Western Parts of the Ottoman Balkans*, "OTAM", No. 34, 2013, pp. 130-132

[9] Bedri Muhadri, *The Invasion of Kosovo from the Ottomans in the XIV Century*, "European Journal of Social Sciences Studies", Vol. 2, No. 6, 2017, p. 17

[10] Marzena Maciulewicz, *Divided Cities. A Case Study of Mitrovica*, University of Warsaw, Warsaw, 2019, pp. 159-62

[11] *Idem*

[12] Ebubekir Ceylan, *The Millet System in the Ottoman Empire*, in Judi Upton Word (Ed.), *New Millenium Perspectives in the Humanities*, Fatih University/Brigham Young University, Global Humanities Press, New York, 2002, pp. 245-266

[13] Bedri Muhadri, *Op. cit*., pp. 18-19

Addressing the divisions in Mitrovica necessitates examining the collapse of the Socialist Federal Republic of Yugoslavia in the early 1990s. The era was characterized by a centrally driven ideology of "brotherhood and unity"[1], coupled with the personality cult surrounding Josif Broz Tito. This ideology served to suppress rising nationalist sentiments among the various ethnic groups. However, this approach ultimately failed as ethnic identities and nationalist movements emerged, fueled by a resurgence of religious feelings within these communities. Following Tito's death, Kosovo faced increasing ethnic tensions, culminating in the revocation of its autonomy in 1989[2]. The response from the Albanian members of the Kosovo Assembly was to declare independence from Serbia in July 1990, which led to a boycott of Serb-dominated institutions by the Albanian community[3]. This escalating conflict between Albanian secessionists and Serbian authorities significantly affected Mitrovica, disrupting its social fabric and ethnic balance. The 1990s saw the rise of democratic elections in Serbia, during which Kosovo Serbs, feeling marginalized, bolstered Slobodan Milošević's nationalist agenda[4]. His hardline rhetoric intensified the conflict, particularly as the Kosovo Liberation Army launched violent campaigns against Serbian police and officials. This turmoil ultimately triggered NATO's intervention in 1999[5]. Following the Kosovo War in 1999 and the 2008 *Declaration of Independence*[6], Mitrovica suffered economic collapse, turning from the economic center of Kosovo before 1999 to the poorest region in Kosovo after 1999.

Nowadays, Mitrovica (located in northern Kosovo about 40 km from Pristina) is split into two distinct parts: the southern region, primarily inhabited by Albanians, operates under the authority of Pristina, where Albanian is the predominant language[7]. This area features Albanian national symbols, mosques, and the euro as its currency. In contrast, the northern region is predominantly populated by Serbs, where Serbian is the most widely spoken language. Here, Serbian national symbols, Orthodox churches, and the Serbian dinar are prevalent. The city's urban landscape is divided into various neighborhoods, each representing distinct cultural and social dynamics, such as the Bosnian and Romani districts. Identifying a city center is complex, as residents' reference multiple locations based on functional significance, including areas near the former Hotel Jadran and the main mosque. The main bridge in Mitrovica serves as a central piece of infrastructure and a critical element of the city's symbolic landscape, representing fragmentation on functional, social, and symbolic levels[8]. Originally constructed in 1884 using stones from the Zvečan fortress, the bridge underwent numerous renovations, the most important ones being the post-war renovations funded by the French government, which took place between 2000-2001. Throughout the time, the bridge's surroundings evolved significantly. Shortly after the *Declaration of Independence*, barricades, hostile graffiti, and the presence of KFOR[9] and Kosovo police characterized the area. In the past few years, the southern side saw significant renovations, revitalizing the riverbanks and encouraging local activity, while the northern side remained under construction but became more accessible. In addition to the main bridge, other prominent landmarks in Mitrovica's symbolic landscape include the monument on the hill, the Orthodox Church, Lazar's monument, the new mosque, and various national symbols.

The pragmatic aspect of division is very complex. The most visible landmark of this division is the physical barrier created by the main bridge, often referred to as French Bridge. This bridge not only physically separates the northern and southern parts of the city but also symbolizes the broader ethnic and cultural schism that characterizes life in Mitrovica. While it stands close to traffic, smaller bridges nearby facilitate limited

[1] Noam Chomsky, *Yugoslavia: Peace, War, and Dissolution*, PM Press, London, 2018, pp. 68-71

[2] Joseph *Marko, The Revocation of the Kosovo Autonomy 1989 – 1991 and Its Consequences for the Idea of European Integration*, Konrad Adenauer Foundation, Pristina, 1999, pp. 17-19

[3] Tim Judah, *Kosovo: What Everyone Needs to Know*, Oxford University Press, London, 2008, p. 43

[4] Noam Chomsky, *Op. cit.*, pp. 68-71

[5] Klaus Naumann, *NATO, Kosovo, and Military Intervention* "Global Governance", Vol. 8, No. 1, 2002, pp. 13-17

[6] *Kosovo's Declaration of Independence,* https://www.refworld.org/legal/legislation/natlegbod/2008/en/56552, (29.10.2024)

[7] Marzena Maciulewicz, *Op.cit.*, pp. 86-89

[8] Kai Voeckler, *Divided Cities and Building Dialogue. Community Centers in Mostar, Mitrovica and Nicosia* in *Urban Transformation in Southeastern Europe*, 2012, pp. 79-83

[9] Tom Gallagher, *The Balkans in the New Millennium: In the Shadow of War and Peace*, Routledge, London, 2005, pp. 57-59

interaction, revealing a community that remains divided yet occasionally engages[1]. Institutionally, Mitrovica is fragmented, with separate municipalities, mayors, and local assemblies governing each side[2]. This dual governance impacts everyday life, from the provision of utilities to the operation of sports teams and schools, which follow different curricula based on ethnicity. Such segregation reflects the broader political climate in Kosovo, where historical grievances and nationalistic sentiments have intensified since the dissolution of Yugoslavia, leading to ongoing tensions between Albanian and Serbian communities[3].

Socially and religiously, the city is marked by distinct identities, with each community maintaining its cultural practices and places of worship. The presence of Serbian Orthodox cemeteries in the south and Muslim Albanian cemeteries in the north further exemplifies this division. Intangible elements, particularly memory and geopolitical allegiance, play a crucial role in perpetuating divisions. Collective memories of past conflicts, displacement, and violence foster a mutual geography of fear among residents. Furthermore, political allegiances shape perspectives on international actors, with NATO viewed favorably by Albanians while Serbs express strong support for Russia and its actions in Crimea and Donbass[4]. Together, these tangible and intangible factors create a pragmatic reality in Mitrovica, where divisions persist despite occasional interactions.

Recent dynamics and escalations in Mitrovica

From the end of the Kosovo War in 1999, Kosovo has encountered periods of intense tension and instability, especially in its inter-ethnic relations and political landscape. A significant escalation occurred in March 2004, when inter-ethnic violence erupted across multiple cities, including Mitrovica, where tensions ran particularly high due to its deep ethnic divisions[5]. Riots primarily targeted Kosovo Serbs, leading to the destruction of homes, churches, and properties, and displacing thousands of people. In Mitrovica, as in other areas, KFOR intervened to protect vulnerable communities, yet the violence underscored the profound ethnic fractures within Kosovo, especially in this divided city[6]. The 2008 *Declaration of Independence* by Kosovo heightened diplomatic conflicts, as Serbia, with support from certain international actors, strongly opposed recognition of Kosovo as an independent state[7]. This event sparked lasting diplomatic and political friction, as Serbia resisted Kosovo's statehood despite recognition from the U.S. and much of the EU. Domestically, Kosovo's governance has faced repeated internal challenges, including political instability and border disputes with Serbia and Montenegro[8]. In Mitrovica, sporadic violence has persisted as an ongoing reminder of unresolved ethnic divides. While EU-mediated talks aim to normalize relations between Kosovo and Serbia, disputes over autonomy for Serb-majority areas, property rights, and the status of the Serbian community remain unresolved, contributing to the complexities of Kosovo's post-war challenges[9].

More recently, in October 2021, Kosovo introduced a "sticker system" following a 13-day blockade of the Jarinje and Brnjak border crossings by Serbian protesters[10]. This blockade stemmed from a longstanding dispute over license plate regulations between Belgrade and Pristina. At the core of the issue was the recognition of each country's license plates; Serbia viewed recognizing Kosovo's plates as a step toward

[1] Jaume Castan Pinos, *Op.cit*., pp. 128-142
[2] Marzena Maciulewicz, *Op.cit*., p. 156
[3] Annika Björkdahl, Ivan Gusic, *Mostar and Mitrovica: Contested Grounds for Peacebuilding*, "Lund University", No. 1, 2013, pp. 22-23
[4] Balkan Insight, *Two Years On. Balkan States Remain Divided Over Ukraine War*, https://balkaninsight.com/2024/02/23/two-years-on-balkan-states-remain-divided-over-ukraine-war/, (30.10.2024)
[5] The Government of the Republic of Serbia, *The March Pogrom (2004)*, https://www.srbija.gov.rs/kosovo-metohija/en/8923 (21.10.2024)
[6] Cristina Deffert, Iuliana Neagoș, *The Necessity and Efficiency of Nato-Led International Peacekeeping Operations in Kosovo After 1999*, "Studia Securitatis", No. 2, 2023, pp. 256-269
[7] Colin Warbrick, *Kosovo: The Declaration of Independence*, "The International and Comparative Law Quarterly", Vol. 57, No. 3, 2008, pp. 675-677
[8] Milena Sterio, *The Case of Kosovo: Self-Determination, Secession, and Statehood Under International Law*, "American Society of International Law", Vol. 104, 2010, pp. 361-365
[9] Bashkim Rrahmani, Majlinda Bregu, *Endless EU Facilitated-Mediated Dialogue Between Kosovo and Serbia*, "Insight Turkey", Vol. 25, No. 1, 2023, pp. 223-246
[10] Mihai Melintei, Cristina Deffert, *The Problem of Free Movement of Means of Transport in the Transnistrian and Kosovo Case*, "Anuarul Laboratorului pentru Analiza Conflictului Transnistrean", Vol. 6, No. 1, 2022, p. 67

acknowledging its independence, while Kosovo asserted its right to reciprocal treatment. To resolve the dispute, Kosovo and Serbia agreed that representatives would meet in Brussels to seek a long-term solution over six months. However, no agreement emerged from these negotiations. International mediators, including the EU, continued efforts to bridge differences, and finally, after extended discussions, an agreement was reached[1]. The compromise required Kosovo Serbs to replace Serbian-issued license plates, which referenced towns within Kosovo, with plates issued by the Republic of Kosovo. This agreement marked an essential step in reducing tensions and resolving the ongoing conflict in northern Kosovo, where many ethnic Serbs reside.

Furthermore, in May 2023, Serbs in northern Kosovo largely boycotted local elections, resulting in victories for ethnic Albanian candidates[2]. This led to confrontations on May 29, when twenty-five NATO peacekeepers were injured during clashes with ethnic Serbs opposing the installation of these mayors[3]. Following these events, Serbian President Aleksandar Vučić placed the Serbian Armed Forces on heightened alert. On June 14, Serbian authorities arrested three Kosovo Police officers, claiming they crossed the border illegally, a charge Kosovo's Prime Minister Albin Kurti disputed, insisting the officers were detained within Kosovo's territory. Furthermore, in June 2023, the Kosovar government designated the Serbian organizations "Civilna Zastita" and "North Brigade" as terrorist groups, citing their involvement in attacks on security forces and public property[4]. While intended to reinforce state control in the north, this move has heightened concerns among Serb communities, with officials like Nenad Rašić warning that such measures could amplify fear and insecurity among local Serbs[5]. The situation escalated with the Banjska attack on September 24, 2023, when Serbian forces clashed with Kosovo police over an unlicensed vehicle, resulting in the death of Kosovo Sergeant Afrim Bunjaku, who was posthumously honored[6]. After the attack, Kosovo police arrested eight individuals, including Serbian Vice President Milan Radoidičić, who accepted responsibility. In response to rising tensions and increased Serbian military presence at the border, NATO reinforced its Kosovo Force with over 130 Romanian troops on October 13 and an additional 200 British soldiers earlier that month[7].

On February 1, 2024, Kosovo imposed a ban on the use of the Serbian dinar, mandating the euro as the sole currency for local transactions[8]. This move has intensified tensions between Belgrade and Pristina, particularly affecting residents in 10 municipalities with significant Serbian populations, including Mitrovica. While Kosovo officials argue that this decision aligns with the constitution's mandate for a single legal currency, many Serbs in Kosovo view it as discriminatory and a violation of their rights. They emphasize that the dinar is commonly used for salaries, pensions, and transactions within Serbian-led institutions like schools and hospitals. In Mitrovica, Serbian protestors condemned the ban, deeming it an infringement on minority rights[9]. This situation followed a contentious UN Security Council meeting, where Kosovo was accused of

---

[1] Anadolu Ajansı, *Serbs in Kosovo End Longstanding Dispute over Vehicle License Plates,* https://www.aa.com.tr/en/europe/serbs-in-kosovo-end-longstanding-dispute-over-vehicle-license-plates/3055090 (25.10.2024)

[2] Reuters, *NATO Soldiers Injured in Kosovo Clashes with Serb Protesters*, https://www.reuters.com/world/europe/nato-soldiers-deploy-around-kosovo-town-halls-standoff-with-serb-protesters-2023-05-29/ (25.10.2024)

[3] BBC, *Kosovo: Why Is Violence Flaring Between Ethnic Serbs and Albanians?*, https://www.bbc.com/news/62382069 (25.10.2024)

[4] Reuters, *Kosovo Designates Two Serb Groups as Terrorist Organizations,* https://www.reuters.com/world/europe/kosovo-designates-two-serb-groups-terrorist-organisations-2023-06-29/ (27.10.2024)

[5] Vijesti, *What Are "Civil Protection" and "Brigade Sever" That Kosovo Wants to Declare as Terrorist Organizations?,* https://en.vijesti.me/world-a/balkan/662842/what-are-the-civil-protection-and-brigade-north-that-kosovo-wants-to-declare-as-terrorist-organizations (27.10.2024)

[6] Al Jazeera, *Kosovo Monastery Siege Ends Following Deadly Attack on Police*, https://www.aljazeera.com/news/2023/9/24/one-police-officer-killed-in-kosovo-attack-blamed-on-serbia (28.10.2024)

[7] Radio Free Europe, *Romania Sends Reinforcements To KFOR In Kosovo, Says NATO*, https://www.rferl.org/a/kosovo-kfor-romanian-reinforcements-nato/32637314.html (28.10.2024)

[8] Voice of America, *Kosovo's Ban on Serbian Dinar Leads to Protests,* https://www.voanews.com/a/kosovo-s-ban-on-serbian-dinar-leads-to-protests-/7484291.html (26.10.2024)

[9] The Guardian, *Kosovo Accused of Raising Ethnic Tensions by Banning Use of Serbian Dinar,* https://www.theguardian.com/world/2024/feb/06/kosovo-accused-of-raising-ethnic-tensions-by-banning-use-of-serbian-dinar (26.10.2024)

blocking a dinar shipment for Serbian pensions and salaries[1]. Prime Minister Albin Kurti defended the ban as a measure against illegal currency flows rather than financial assistance from Serbia.

In addition, in August 2024, Kosovo President Vjosa Osmani has expressed concerns that reopening the Mitrovica bridge to traffic without coordination with NATO could lead to clashes between Kosovo police and U.S. troops[2]. The bridge, closed since the end of the Kosovo War in 1999, has been the site of severe ethnic violence between Albanians and the predominantly Serbian population in northern Kosovo. Its reopening would be a significant gesture, even as three other bridges already span the river. Osmani emphasized that a conflict between local authorities and U.S. forces is not in Kosovo's interest, highlighting the importance of maintaining peace in the region[3]. Nevertheless, the bridge, once used as a military checkpoint and de facto border, has been open to pedestrians since the post-war renovations were completed and can be crossed freely, without controls, under normal conditions of social and political stability. In case of escalations, access to the bridge was temporarily interrupted[4]. Since 2012, Italian Carabinieri from KFOR and the Kosovo Police have maintained a continuous presence on both ends of the bridge to ensure peace and deter illegal activities.

Furthermore, on September 2, 2024, protests erupted in North Mitrovica after Kosovo authorities shut down five Serbia-run "parallel institutions" in the Serb-majority north[5]. The closure followed raids by Kosovo Police on Serbia-backed facilities, suspected of issuing falsified documents. Around 70-80 Kosovo Serbs gathered to protest the closure of the parallel municipality office. Kosovo's actions were criticized by Western diplomats, including US Ambassador Jeffrey Hovenier, who warned that such uncoordinated moves could escalate tensions, threaten safety, and damage Kosovo's reputation as a reliable international partner, particularly regarding relations with its Serb community[6]. Henceforth, on September 7, 2024, Kosovo's government announced the closure of two of its four border crossings with Serbia, specifically the Brnjak and Merdare crossings[7]. This decision followed protests on the Serbian side, where demonstrators obstructed roads and refused passage to individuals presenting Kosovo-issued documents. Kosovar Interior Minister Xhelal Svecla attributed the closures to the actions of "masked extremist groups in Serbia" that were selectively impeding transit for travelers[8]. He emphasized that these activities occurred under the watch of Serbian authorities.

Thus, the situation in Mitrovica is constantly determined by this division, and every time there is an escalation of ethnic tensions, the theater of actions will always be the northern part of Kosovo and mainly Mitrovica, because it is the most volatile area, where the lack of urban cohesion makes it prone to violence and degradation of human security.

Concluding remarks

All in all, Mitrovica stands as a vivid symbol of the ongoing complexities that shape Kosovo's socio-political landscape. The divisions within Mitrovica today are not just about geography but are rooted in a long history of ethnic tensions, national identities, and conflicting political allegiances. The physical division,

---

[1] ONU, *Security Council Debates Kosovo's New Rules on Serbian Currency*, https://news.un.org/en/story/2024/02/1146382 (16.02.2024)

[2] Reuters, *Opening Kosovo's Mitrovica Bridge Risks Conflict with US Troops, Says President,* https://www.reuters.com/world/opening-kosovos-mitrovica-bridge-risks-conflict-with-us-troops-says-president-2024-08-15/ (30.10.2024)

[3] Radio Free Europe, *Reopening of Mitrovica Bridge Long Overdue but Must Be Done in Consultation with Allies, Says Kosovo's President,* https://www.rferl.org/a/kosovo-serbia-osmani-mitrovica-bridge-kurti-vucic/33084758.html (30.10.2024)

[4] Marzena Maciulewicz, *Op. cit*., p. 97

[5] Balkan Insight, *Kosovo Serbs Protest Closure of Serbia-Run 'Parallel Institutions',* https://balkaninsight.com/2024/09/02/kosovo-serbs-protest-closure-of-serbia-run-parallel-institutions/, (02.11.2024)

[6] *Idem*

[7] Al Jazeera, *Kosovo Closes Two of Four Border Crossings with Serbia After Protests,* https://www.aljazeera.com/news/2024/9/7/kosovo-closes-two-of-four-border-crossings-with-serbia-after-protests (02.11.2024)

[8] Reuters, *Kosovo Closes Two Border Crossings with Serbia After Protest*, https://www.reuters.com/world/europe/kosovo-closes-two-border-crossings-with-serbia-after-protest-2024-09-07/ (02.11.2024)

symbolized by the main bridge that separates the northern and southern parts of the city, mirrors the fragmented nature of its society, where both Albanians and Serbs continue to live in parallel realities. The challenges that Mitrovica faces are not unique to the city itself but are part of a larger struggle within Kosovo to reconcile its past and build a shared future. While efforts to establish a cohesive, inclusive state have been made, the region remains deeply divided by memories of conflict and fears of the future. Political decisions continue to steady these divisions, creating moments of tension that threaten to escalate into violence.

In the paradigm of human security, the separation of the two communities significantly affects freedom of movement, freedom of political and religious expression, freedom of assembly. In the absence of natural economic and social relations, instead of a homogeneous community, we are witnessing major disruptions in communication and development and the perpetuation of the singularization phenomenon. Any program to resolve the protracted crisis in the case of Mitrovica should be written through chapters and sub-chapters addressed to the above themes, for which we identify causes and solutions.

What seems clear is that the future of Mitrovica depends on more than just political agreements or border negotiations. It requires the rebuilding of trust between communities, a careful balance between state sovereignty and local autonomy, and the sustained involvement of international mediators to ensure that peace remains fragile, but intact. The road ahead is uncertain, but the ongoing efforts to find common ground, both within Mitrovica and across Kosovo, are essential in creating a future where division no longer defines the city, or the nation.

Bibliography

Books

1. Chomsky, Noam, *Yugoslavia: Peace, War, and Dissolution*, PM Press, London, 2018
2. Gallagher, Tom, *The Balkans in the New Millennium: In the Shadow of War and Peace*, Routledge, Londra, 2005
3. Judah, Tim, *Kosovo: What Everyone Needs to Know*, Oxford University Press, Londra, 2008
4. Malcolm, Noel, *Kosovo: A Short History*, Harper Collins, New York, 1998
5. Marzena Maciulewicz, *Divided Cities. A Case Study of Mitrovica*, University of Warsaw, Warsaw, 2019

Studies and Articles

1. Björkdahl, Annika; Gusic, Ivan, *Mostar and Mitrovica: Constested Grounds for Peacebuilding*, "Lund University", No. 1, 2013
2. Ceylan, Ebubekir, *The Millet System in the Ottoman Empire*, in Judi Upton Word (Ed.), *New Millenium Perspectives in the Humanities*, Fatih University/Brigham Young University, Global Humanities Press, New York, 2002
3. Deffert, Cristina; Neagoș, Iuliana, *The Necessity and Efficiency of Nato-Led International Peacekeeping Operations in Kosovo After 1999*, "Studia Securitatis", No. 2, 2023
4. Kursar, Vjeran, *Being an Ottoman Vlach: On Vlach Identity (Ies), Role and Status in Western Parts of the Ottoman Balkans*, "OTAM", No. 34, 2013
5. Marko, Joseph, *The Revocation of the Kosovo Autonomy 1989 – 1991 and Its Consequences for the Idea of European Integration*, Konrad Adenauer Foundation, Pristina, 1999
6. Melintei, Mihai; Deffert, Cristina, *The Problem of Free Movement of Means of Transport in the Transnistrian and Kosovo Case*, "Anuarul Laboratorului pentru Analiza Conflictului Transnistrean", Vol. 6, No. 1, 2022
7. Muhadri, Bedri, *The Invasion of Kosovo from the Ottomans in the XIV* Century, "European Journal of Social Sciences Studies", Vol. 2, No. 6, 2017
8. Naumann, Klaus, *NATO, Kosovo, and Military Intervention*, "Global Governance", Vol. 8, No. 1, 2002
9. Pinos, Jaume Castan, *Mitrovica: A City (Re)Shaped by Division*, "Politics of Identity", Vol. 29, No. 9, 2015
10. Rrahmani, Bashkim; Bregu, Majlinda, *Endless EU Facilitated-Mediated Dialogue Between Kosovo and Serbia*, "Insight Turkey", Vol. 25, No. 1, 2023
11. Sterio, Milena, *The Case of Kosovo: Self-Determination, Secession, and Statehood Under International Law*, "American Society of International Law", Vol. 104, 2010

12. Warbrick, Colin, *Kosovo: The Declaration of* Independence, "The International and Comparative Law Quarterly", Vol, 57, No, 3, 2008
13. Yannis, Alexandros, *The UN as Government in Kosovo*, "Global Governance", No. 1, 2004
14. Voeckler, Kai, *Divided Cities and Building Dialogue. Community Centers in Mostar, Mitrovica and Nicosia*, "Urban Transformation in Southeastern Europe", 2012

Websites

1. https://balkaninsight.com
2. https://en.vijesti.me
3. https://news.un.org
4. https://www.aljazeera.com
5. https://www.eulex-kosovo.eu
6. https://www.euractiv.com
7. https://www.nato.int
8. https://www.reuters.com
9. https://www.srbija.gov.rs
10. https://www.theguardian.com

Andreea-Nicoleta DRAGOMIR (1)
Lucian Blaga University of Sibiu, Romania
Ana MORARI (BAYRAKTAR) (2)
Lucian Blaga University of Sibiu, Romania

THE ROLE OF TECHNOLOGY IN MIGRATION MANAGEMENT. BALANCING SECURITY, ETHICS, AND HUMAN RIGHTS

Abstract:	*In the context of increasing migration and refugee flows, the integration of new advanced technologies into border security and their implications for human security requires considerable adjustment. AI-driven surveillance, biometric identification, and automated controls at the border have become part of strategic security measures. While these technologies seek to create "smart borders" for effective functionality, major concerns are raised for data privacy and civil liberties, and the potential for discriminatory practices against vulnerable populations.* *The analysis describes ethical and humanitarian dilemmas created by the technologization of border management concerning issues for access to international protection by asylum seekers under the 1951 Refugee Convention. It does so by drawing on comparative case studies from the member states of the European Union, illustrating how different geopolitical contexts shape the deployment and regulation of those technologies. This research calls for a balanced policy approach that incorporates the notion of border security with the principles of international human rights law, thereby advancing a framework that protects the dignity and rights of all individuals.*
Keywords:	**Migration; human security; smart borders; refugee**
Contact details of the authors:	E-mail: andreea.dragomir@ulbsibiu.ro (1) ana.morari@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Lucian Blaga University of Sibiu, Faculty of Law (1) (2)**
Institutions address:	Calea Dumbrăvii 34, Sibiu, Romania 550324 (1) (2)

Introduction

Migration management is fast assuming new dimensions, with advanced technologies taking center stage in the processes of border control worldwide. Added to protect against illegal migration and verify the identity of aliens and migrants, they raise difficult questions about their legal and ethical implications. A critical tension seems to arise between the need for strong measures of security and the imperatives of human rights to be upheld, including privacy, non-discrimination, and freedom of movement.

Enhanced migration is also impelling state and non-state actors to use ADT in innovative management frameworks. Abstract data use refers to the concept of abstract data types (ADTs), which are mathematical models that define data types based on their behavior rather than their implementation. A queue ADT can be used to handle the incoming traveler data in the order it is received hence ensuring efficiency in the processing at border checkpoints. When a traveler presents their identification, the system can rapidly carry out operations such as searching for alerts or verifying biometric information without exposing the underlying complexities of these processes[1].

The mechanism to manage the problems related to the massive influx of refugees and migrants, due to a political or economic connection in the state of origin, has increased the need to implement digital tools

[1] Yingxu Wang, Xinming Tan, Cyprian Ngolah, Philip Sheu, *The Formal Design Models of a Set of Abstract Data Types (ADTs)*, "International Journal of Software Science and Computational Intelligence (IJSSCI)", Vol. 2, No. 4, 2010, pp. 72-100, https://doi.org/10.4018/jssci.2010100106 (30.10.2024)

capable of facilitating the exchange of information between agents, from artificial intelligence to other systems based on blockchain, web 3.0. RPA, etc.[1].

As a result, for example, the identity, visa status, and customs declarations of travelers can be stored on a blockchain, which unauthorized persons will find very difficult to alter. The unchangeable nature of blockchain means that once information is added, it cannot be changed without agreement from the network[2].

In the same way, Robotic Process Automation (RPA), a technology that automates repetitive, rule-based tasks commonly performed by humans using software robots or *bots*, can integrate data coming from different sources and systems without major infrastructure changes[3]. It can draw information from different databases—be it traveler records, security alerts, or even customs information—and present a single view of the information to the border officials[4].

Technological adaptations-from biometric systems and AI-driven surveillance to remote sensors and data analytics-aim to bolster border security and streamline migration processes[5].

As much as these technologies enhance security and efficiency, there are still concerns about their accuracy, especially in real situations where demographic diversity interferes with their efficacy. These potential negative impacts include biased outcomes, data privacy problems, systemic inequities, and transparency deficits-issues identified by stakeholders, especially within communities with historic disadvantages[6].

"Smart borders" - errosion of due process

Smart borders have as part of their core highly innovative digital border technologies, from simple internet-enabled devices to advanced systems powered by algorithms, AI, and AD. Examples include machine learning, predictive analytics, facial recognition systems, biometric databases, drones, and other forms of surveillance mechanisms. Their integration furthers and optimizes the efficiency of border management[7].

The increasing integration of digital technologies in border governance and their implications for migration politics highlights how states and private actors employ tools such as big data analytics and automated decision-making systems in border management. These technologies are utilized in identification documents, facial recognition systems, biometric databases, and surveillance mechanisms, aiming to enhance efficiency and security[8].

Such smart border systems use biometric technologies for more accurate identification and verification of travelers through face recognition, fingerprints, or iris scans. Biometrics integrated with the border control

---

[1] Giuli Giguashvili, *Possibilities of Using Artificial Intelligence in the Process of International Migration Management*, "Innovative economics and management", Vol. 10, No. 3, 2023, https://doi.org/10.46361/2449-2604.10.3.2023.58-66 (30.10.2024)

[2] Sanket Panchamia, Deepak Kumar Byrappa, *Passport, VISA and Immigration Management Using Blockchain*, "2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)", 2017, pp. 8-17 https://doi.org/10.1109/ADCOM.2017.00009, (30.10.2024)

[3] Hema G.B. Malini, *Automation of Big Data Analytics Using Robotic Process Automation*, "International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)", Vol. 7, No. 2, 2021, pp. 602-605, https://doi.org/10.32628/CSEIT2172124 (30.10.2024)

[4] Georgios Glouftsios, *Governing border security infrastructures: Maintaining large-scale information systems*, "Security Dialogue", Vol. 52, No. 5, 2020, pp. 452 – 470, https://doi.org/10.1177/0967010620957230 (30.10.2024)

[5] Bruno Oliveira Martins, Maria Gabrielsen Jumbert, *EU Border technologies and the co-production of security 'problems' and 'solutions'*, "Journal of Ethnic and Migration Studies", 48, 2020, pp. 1430-1447, https://doi.org/10.1080/1369183X.2020.1851470 (30.10.2024)

[6] United States Government Accountability Office, *Biometric Identification Technologies Considerations to Address Information Gaps and Other Stakeholder Concerns*, Report to Congressional Committees, 2024, https://www.gao.gov/assets/gao-24-106293.pdf (30.10.2024)

[7] Lorna McGregor, Petra Molnar, *Digital Border Governance: A human rights based approach*, Online Study University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023, p. 8, https://repository.essex.ac.uk/36656/1/Digital%20Border%20Governance%20-%20A%20Human%20Rights%20Based%20Approach.pdf (30.10.2024)

[8] Natasha Saunders, *Security, digital border technologies, and immigration admissions: Challenges of and to non-discrimination, liberty and equality*, "European Journal of Political Theory", 2023 https://doi.org/10.1177/14748851231203912 (30.10.2024)

system allow, under different EU initiatives such as the *Smart Borders Policy*, an automated entry/exit system with more reliability of data. These systems have been integrated with various frameworks, for instance, the *Schengen Border Code (SBC)*, allowing operations to proceed smoothly without compromising on the security level[1].

Smart borders have a reliance on biometric systems, which include facial recognition systems, that create a variety of risks. For example, Clearview AI scraped billions of images online to use in unauthorized facial recognition, while a breach at U.S. Customs exposed 100,000 facial images. It was reported that "studies had found facial recognition algorithms misidentify people of certain races at rates as much as ten times higher than others, with new concerns about discrimination"[2].

Furthermore, the systems exclude users who have disabilities or low technology literacy. Although laws such as the GDPR and some others regulate biometric data, inconsistent enforcement leaves gaps in privacy and accountability. These risks need to be addressed in a solution to make border management both ethical and secure[3].

The performance and usefulness of smart borders are unquestionable, however raises concerns about the lack of transparency and accountability in deploying these digital border technologies. Limited public information is available regarding their use, often justified by states on grounds of national security and sovereignty. This opacity is further compounded when private actors are involved, consolidating knowledge and power within the private sector and hindering oversight[4].

In response to these concerns, at the EU level, a pilot project has been set up to study and technically support operational systems involved in smart borders technology, with the aim of answering questions about their cost-effectiveness, reliability, and impact on fundamental rights. While at least at a technical level data security is provided some form of protection through this program, the lack of legal regulation raises concerns that critical decisions are being made in a way that bypasses meaningful public debate, limiting opportunities for citizens, civil society and legislators to scrutinize and shape the direction of these initiatives[5].

Legal initiatives to regulate data sharing

The EU has increasingly applied digital systems to monitor, regulate, and control the flows of migration, changing how migration has been traditionally regulated within its member states. These systems are meant to enhance border security and administrative efficiency while making it easier to identify and track who is crossing in and out of territories[6].

Schengen information system

The Schengen Information System is the EU's largest information-sharing platform, which is indispensable in the management of borders and assurance of security within the Schengen Area[7]. In place since 1995 and, in its second generation, since 2013, the SIS has so far allowed member states and associated

[1] Mohamed Abomhara, Sule YildirimYayilgan, Livinus ObioraNweke, ZoltánSzékely, *A comparison of primary stakeholders'views on the deployment of biometric technologies in border management: Case study of SMart mobILity at the European land borders*, Technology in Society", Vol. 64, February, 2021, https://doi.org/10.1016/J.TECHSOC.2020.101484 (30.10.2024)

[2] Blaž Meden, Peter Rot, Philipp Terhörst et al., *Privacy–Enhancing Face Biometrics: A Comprehensive Survey*, "IEEE Transactions on Information Forensics and Security", Vol. 16, 2021 https://ieeexplore.ieee.org/ielx7/10206/9151439/09481149.pdf (01.11.2024)

[3] *Idem*

[4] Natasha Saunders, *Op. cCit.*, pp.10-12

[5] Didier Bigo, Julien Jeandesboz, Jorrit Rijpma, *Smart Borders Revisited: An Assessment of the Commission's Revised Smart Borders Proposal*, "European Parlement Research Report", November 2016, p. 52 https://sciencespo.hal.science/hal-03459136v1/document (30.10.2024)

[6] Bruno Oliveira Martins, Kristoffer Lidén, Maria Gabrielsen Jumbert, *Border security and the digitalization of sovereignty: insights from EU borderwork*, "European Security", Vol. 31, No. 3, 2022, pp. 475-494 https://doi.org/10.1080/09662839.2022.2101884 (30.10.2024)

[7] European Commission, *Schengen Information System*, https://home-.affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en (30.10.2024)

countries to share, in real-time, alerts on persons and objects-a missing person, a stolen vehicle, or a fraudulent document[1].

As of 2023, the system knows new alert categories and improved information processing. This SIS contains biometric data, such as fingerprints and photographs of people, to increase the correct identification of people at border control or in police services[2]. Specific rights linked to transparency and given to individuals have always represented one of the main modalities in which SIS develops this concept. According to SIS II legal regulations, such people also acquire rights to have access, correctness with some elements, and lawful deletion regarding the data of the owner that has been processed through this system[3].

Several mechanisms put SIS at responsibility: The Schengen Evaluation and Monitoring Mechanism provides for regular assessment to be carried out by the Commission on the implementation of member states regarding the Schengen acquis[4].

The respective EU data protection laws binding SIS on the collection, storage, and exchange of personal data, including special legislation contained within the Schengen Convention, regard the personal data as sensitive information, including biometric identifiers, available only to the competent authority authorized and then only when it is strictly necessary for a legitimate end. Each participating state will have an established and independent body known as the National Supervisory Authority responsible for overseeing this area of law to deter and discuss any misuse of the data[5].

Visa information system (VIS)

The Visa Information System is a central database allowing the Schengen States to exchange visa information, thus supporting the implementation of the European Union's common visa policy. It connects consulates based in non-EU countries with all external border crossing points of the Schengen States, managing data and decisions related to short-stay visa applications for persons planning to visit or transit through the Schengen Area.

One of the most important features of VIS is the possibility to prevent "visa shopping" by allowing member states to detect and stop any further applications following a rejection[6]. It also supports asylum procedures by helping to identify the state responsible under the Dublin Regulation by checking the visa history records. Additionally, VIS helps law enforcement in investigating serious crimes, including terrorism, subject to strict legal conditions[7].

EURODAC (European Asylum Dactyloscopy Database)

The European Asylum Dactyloscopy Database (EURODAC) is a centralized system established in 2003 to streamline asylum application processes within the EU and associated countries. It plays a pivotal role in supporting the implementation of the Dublin Regulation, which determines the EU Member State responsible for examining an individual's asylum application[8].

---

[1] Izabella Majcher, *The Schengen-wide entry ban: how are non-citizens' personal data protected?*, "Journal of Ethnic and Migration Studies", Vol. 48, 2020, pp. 1944 – 1960 https://doi.org/10.1080/1369183X.2020.1796279 (01.11.2024)

[2] European Commission, *What is SIS and how does it work?*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en (01.11.2024)

[3] Christian Janssen, Jonas Kathmann, *Legal Requirement Elicitation, Analysis and Specification for a Data Transparency System.*, Springer Nature Link, 2020, pp. 3-17, https://doi.org/10.1007/978-3-030-53337-3_1 (01.11.2024)

[4] EU Monitor, Annexes to COM (2020)779 - Functioning of the Schengen Evaluation and Monitoring Mechanism under Article 22 of Council Regulation (EU) No. 1053, 2013, https://www.eumonitor.eu/9353000/1/j4nvirkkkr58fyw_j9vvik7m1c3gyxp/vle2l9lttgzy (01.11.2024)

[5] Sebastian Kaniewski, *Genesis And Significance Of The Schengen Information System (SIS)*, "Edukacja Humanistyczna", Vol. 2, No. 33, 2015, pp. 89-96, https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-f24892b7-07af-49b9-b6e2-cdac93f96390 (01.11.2024)

[6] Georgios Glouftsios, Stephan Scheel, *An inquiry into the digitization of border and migration management: performativity, contestation and heterogeneous engineering*, Third World Quarterly", No. 42, 2020, pp. 123-140 https://doi.org/10.1080/01436597.2020.1807929 (01.11.2024)

[7] *Idem*

[8] European Commission, *EURODAC (European Asylum Dactyloscopy Database)*, 2022, https://knowledge4policy.ec.europa.eu/dataset/ds00008_en (01.11.2024)

By collecting and comparing fingerprint data, EURODAC ensures consistency and fairness in processing applications while preventing multiple submissions in different countries[1]. The revised EURODAC regulation introduces important changes in migration governance. The age threshold for taking fingerprints has been lowered from 14 to 6 years. The system has been upgraded with the inclusion of facial images and biometric details[2].

The EU's adoption of digital systems like SIS, VIS, and EURODAC has modernized migration management, improving border security, administrative efficiency, and tracking capabilities.

Human security risks

Privacy and data protection

One of the most serious problems linked to reinforcing borders with advanced digital technologies is what mechanism exists to balance enhanced security with respect for human rights. Ai-driven surveillance, collection of biometric data, and predictive analytics can be quite powerful means of managing migration flows. Meanwhile, these are susceptible to raising serious concerns about over-surveillance, racial profiling, and erosion of privacy rights[3].

A report in 2018 noted the vulnerabilities of the Schengen Information System (SIS), with insufficient encryption measures, exposing personal data breaches[4]. The use of drone AI cameras in countries like Hungary and Greece to monitor migrant movements has been criticized as a means of racial profiling and a violation of data privacy laws[5].

The 2019 breach of Bulgaria's National Revenue Agency database, which exposed sensitive personal data of nearly 5 million citizens, is an exceptional example of how centralized systems can be hacked[6]. Mechanisms must therefore be in place to ensure that the deployment of new technologies is in line with obligations under international human rights. Underlining this, the OSCE Office for Democratic Institutions and Human Rights (ODIHR) stresses the importance of integrating human rights considerations into the development and use of border technologies by guaranteeing strong legislative frameworks, independent oversight mechanisms, and impact assessments during technology development[7].

Moreover, independent oversight mechanisms should be in place to monitor the use of surveillance technologies at borders. Training border personnel in human rights standards can help ensure that these technologies are used responsibly and ethically. Otherwise, there is a chance that automated decision-making will result in discrimination against asylum seekers and refugees, further increasing systemic inequalities.

Discrimination

Automated profiling mechanism at borders causes discriminatory situations, disproportionately affecting migrants and refugees.

The Federal Anti-Discrimination Agency in its recent expert report, highlights that the use of algorithms in border control often relies on datasets that reflect existing social disparities, which in turn lead to biased outcomes. Profiling mechanisms in European Union border operations are more likely to target people

[1] European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Eurodac statistics, https://data.europa.eu/data/datasets/eurodac-statistics?locale=en (01.11.2024)

[2] Niovi Vavoula, *The Transformation of Eurodac from an Asylum Tool into an Immigration Database*, "EU Immigration and Asylum Law and Policy", 2024, https://eumigrationlawblog.eu/the-transformation-of-eurodac-from-an-asylum-tool-into-an-immigration-database/ (01.11.2024)

[3] Mirko Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, in "BioLaw Journal –Rivista di BioDiritto", No.2, 2021, pp. 433-451, https://doi.org/10.15168/2284-4503-833 (01.11.2024)

[4] Freddy S. Singaraj, *Shroud of Surveillance and Its Threat to Fundamental Rights and Civil Liberties*, "Journal of Emerging Technologies and Innovative Research", 2019, https://www.jetir.org/papers/JETIRBH06007.pdf (01.11.2024)

[5] Panagiotis Loukinas, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, "Surveillance and Society", Vol. 15, No. 3/4, 2017, pp. 439-446, https://doi.org/10.24908/SS.V15I3/4.6613 (02.11.2024)

[6] Georgios Glouftsios, Stephan Scheel, *An inquiry into the digitization of border and migration management: performativity, contestation and heterogeneous engineering*, "Third World Quarterly", No. 42, 2020, pp. 123-140, https://doi.org/10.1080/01436597.2020.1807929 (01.11.2024)

[7] Gemma Galdon Clavell, *Protect rights at automated borders,* "Nature", No. 543, 2017, pp. 34-36, https://doi.org/10.1038/543034a (01.11.2024)

of African and Middle Eastern descent as security threats based on historical trends, rather than analyzing individual behavior[1].

Algorithmic profiling creates spurious classifications, like a "risky population", based on correlations within changing datasets using variables such as income or postal codes rather than protected attributes which makes discrimination much harder to detect[2]. Strong data governance mechanisms form the backbone for managing this sensitive information within AI systems. Organizations should perform Privacy Impact Assessments to consider and alleviate potential risks to individuals regarding the deployment of these technologies. The proactive approach will help them find loopholes in data handling practices, ensuring full transparency under the GDPR regarding how data will be used[3].

Therefore, in the implementation of AI algorithms or automated digital systems in the management of data flow at borders, it is necessary to adopt a legal framework capable of eliminating the consequences of discrimination of a system that builds its image because of bias or innocuous data.

Non-refoulement breaches

Automated border systems may even designate individuals for deportation without proper consideration of asylum applications or the risks they may face in their home countries. The difficulty with this lies in reliance upon biometric and digital technologies that might not engage with the messy particularities of individual situations.

The breaches of non-refoulement are more visible in the EU with the emergence of *digital pushbacks* – a process where information systems are being misused to perpetuate asylum rights violations[4]. The case law on the CJEU on art. 47 of the EU Charter requires deep scrutiny of SIS alerts; however, constraints in national judicial systems impede proper cross-border examination. As a result, migrants often struggle with no means to challenge such alerts, compromising their right to fair asylum procedures[5].

Technologies like iBorderCtrl developed to determine credibility, and AI-driven systems put into use in Germany for determining the origins of asylum seekers are criticized for keeping old discriminations and marginalization alive, possibly violating the non-refoulement principle. While projects like GeoMatch and AI-based mobile solutions aim to support refugees, their misuse by states or malicious actors could endanger asylum seekers[6].

Technological failures, such as app crashes and errors in geolocation, have excluded many migrants without smartphones or access to the internet, disproportionately affecting Black migrants and Haitians due to facial recognition biases and language barriers[7]. These issues effectively denied protection to vulnerable people, in effect violating international law in potentially exposing them to refoulement.

Study Case

Greece's use of AI-powered surveillance at borders

Greece's use of AI-powered surveillance at its borders represents a significant shift in migration management, especially at the Evros land border with Turkey.

---

[1] Carsten Orwat, *Risks of Discrimination through the Use of Algorithms*, Federal Anti-Discrimination Agency, Institute for Technology Assessment and Systems Analysis (ITAS), 2019, https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/EN/publikationen/Studie_en_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.pdf?__blob=publicationFile&v=2 (04.11.2021)

[2] Monique Mann, Tobias Matzner, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, "Big Data&Society", Vol. 6, No.2, 2019, https://doi.org/10.1177/2053951719895805 (04.11.2021)

[3] Yordanka Ivanova, *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI.*, "Materials Performance eJournal", 2020, https://doi.org/10.2139/ssrn.3584219 (04.11.2021)

[4] Romain Lanneau, *Digital pushbacks at European borders: an ongoing threat to the rule of law in the Schengen area*, "Cahiers de l'EDEM", Special Issue, August, 2022, pp. 63-69, https://uclouvain.be/fr/instituts-recherche/juri/cedie/actualites/lanneauaout2022.html (04.11.2021)

[5] *Idem*

[6] *Idem*

[7] Austin Kocher, *Glitches in the Digitization of Asylum: How CBP One Turns Migrants' Smartphones into Mobile Borders*, "Societies 2023", Vol.13, No.6, 2023, p. 149, https://doi.org/10.3390/soc13060149 (04.12.2024)

These policies are deeply rooted in the historical context of exclusionary nationalism in Greece, which defines migrants (predominantly from Muslim countries) as the "Other", associating them with perceived security threats and cultural differences[1].

Following the 2015 migrant crisis, in which more than 850.000 people arrived in Greece, this nation implemented several legislative, political, and technological initiatives to lower migration with EU assistance. These included the blocking of the blocking of the Western-Balkan route, the *EU-Turkey Agreement* for the return of illegal migrants, and joint NATO operations[2].

Greek authorities' actions, which have been widely denounced as pushbacks, have drawn significant international criticism following the tragic deaths of 12 migrants in February 2022 due to freezing temperatures at the Turkish border, illustrating the gravity of these practices. These actions, as stated in art. 33 of the Refugee Convention, which prohibits sending individuals to locations where they could be in danger of persecution, is clearly against the principle of non-refoulement[3].

Coupled with these technological systems in Greece are aggressive pushback strategies that include denial of access to asylum, mass deportations, and endangerment of migrants' lives. While the border laws of Greece claim to align with EU legal frameworks like the *Schengen Borders Code*, the integration of artificial intelligence into an already racially prejudiced and violent border regime further escalates the tension between sovereignty, security, and human rights.

Conclusions

These technologies often coincide in settings where basic rights, like non-refoulement and discrimination, are frequently being breached. Greek border control strategies demonstrate how utilizing advanced technology can exacerbate preexisting racial prejudices and inequities, particularly when combined with forceful actions like pushbacks.

Relying only on AI-driven tools without legal protections and transparency can disrupt the balance between sovereignty and human rights, putting at risk vulnerable migrant populations by marginalizing and endangering them. Strong supervision, strict legal structures, and active public monitoring will ensure that technological changes in border control are used effectively while still respecting human dignity and basic freedoms. The commitment to ensuring safe and ethical migration governance will remain an unattainable goal without the implementation of these measures**.**

A pragmatic conclusion is that while technology can improve border management, it must be implemented with strict oversight and in compliance with international human rights standards. This includes ensuring transparency in how data is collected and used, safeguarding against bias in automated systems, and protecting the rights of vulnerable populations. Effective migration management in an era of technological progress requires a careful balance between strengthening security measures and upholding fundamental human rights.

Bibliography

Books

1. Hemat, Lise, Endregard, '*Just' Research: A Case Study of EU-funded Research with Experimental Artificial Intelligence Technology for Border Control*, The Peace Research Institute Oslo (PRIO), Oslo, 2022

[1] Lena Karamanidou, Bernd Kasparek, *From Exception to Extra-Legal Normality: Pushbacks and Racist State Violence Against People Crossing the Greek–Turkish Land Border*, "State Crime Journal", Vol. 11, No. 1, Special Issue on Migration and Racist State Violence, 2022, pp. 12-32, https://www.jstor.org/stable/48675911, (04.12.2024)

[2] Panagiotis Loukinas, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, "Surveillance and Society", Vol. 15, No. 3/4, 2017, pp. 439-446, https://doi.org/10.24908/SS.V15I3/4.6613 (02.11.2024)

[3] Lise Endregard Hemat, *'Just' Research: A Case Study of EU-funded Research with Experimental Artificial Intelligence Technology for Border Control*, The Peace Research Institute Oslo (PRIO), 2022, https://www.prio.org/publications/13182 (04.12.2024)

2. McGregor, Lorna; Molnar, Petra, *Digital Border Governance: A human rights-based approach*, Online Study University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023

Studies and Articles

1. Abomhara, Mohamed; Yayilgan, Sule, Yildirim; Nweke, Livinus, Obiora; Székely, Zoltán, *A comparison of primary stakeholders'views on the deployment of biometric technologies in border management: Case study of SMart mobILity at the borders*, "Technology European land in Society", Vol. 64, February 2021, https://doi.org/10.1016/J.TECHSOC.2020.101484
2. Bigo, Didier; Jeandesboz, Julien; Rijpma, Jorrit, *Smart Borders Revisited: An Assessment of the Commission's Revised Smart Borders Proposal*, "European Parlement Research Report", 2016, hal-03459136f, https://sciencespo.hal.science/hal-03459136v1/document
3. Clavell Gemma Galdon, *Protect rights at automated borders*, "Nature", No. 543, 2017, https://doi.org/10.1038/543034a
4. Forti, Mirko, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, "BioLaw Journal –Rivista di BioDiritto", No. 2, 2021, https://doi.org/10.15168/2284-4503-833
5. Giguashvili Giuli, Possibilities of Using Artificial Intelligence in the Process of International Migration Management, "Innovative Eeconomics and Management", Vol. 10, No. 3, 2023, https://doi.org/10.46361/2449-2604.10.3.2023.58-66
6. Glouftsios, Georgios, *Governing border security infrastructures: Maintaining large-scale information systems*, "Security Dialogue", Vol. 52, No. 5, 2020, https://doi.org/10.1177/0967010620957230
7. Glouftsios, Georgios; Scheel Stephan, *An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering*, "Third World Quarterly", No. 42, 2020, https://doi.org/10.1080/01436597.2020.1807929
8. Ivanova Yordanka, *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI*, "Materials Performance eJournal", 2020, https://doi.org/10.2139/ssrn.3584219
9. Janssen Christian, Kathmann Jonas, *Legal Requirement Elicitation, Analysis and Specification for a Data Transparency System*, Springer Nature Link, 2020, https://doi.org/10.1007/978-3-030-53337-3_1
10. Kaniewski, Sebastian, *Genesis and Significance of the Schengen Information System (SIS)*, "Edukacja Humanistyczna", Vol. 2, No. 33, 2015
11. Karamanidou, Lena; Kasparek, Bernd, *From Exception to Extra-Legal Normality: Pushbacks and Racist State Violence Against People Crossing the Greek–Turkish Land Border*, "State Crime Journal", Vol. 11, No. 1, Special Issue on Migration and Racist State Violence, 2022, https://www.jstor.org/stable/48675911
12. Kocher, Austin, *Glitches in the Digitization of Asylum: How CBP One Turns Migrants' Smartphones into Mobile Borders*, "Societies 2023", Vol. 13, No. 6, 2023, https://doi.org/10.3390/soc13060149
13. Lanneau, Romain, *Digital pushbacks at European borders: an ongoing threat to the rule of law in the Schengen area*, "Cahiers de l'EDEM", Special Issue, August 2022, https://uclouvain.be/fr/instituts-recherche/juri/cedie/actualites/lanneauaout2022.html
14. Loukinas, Panagiotis, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, "Surveillance And Society", Vol. 15, No. 3/4, 2017, https://doi.org/10.24908/SS.V15I3/4.6613
15. Majcher, Izabella, *The Schengen-wide entry ban: how are non-citizens' personal data protected?*, "Journal of Ethnic and Migration Studies", Vol. 48, 2020, https://doi.org/10.1080/1369183X.2020.1796279
16. Malini Hema G.B., *Automation of Big Data Analytics Using Robotic Process Automation*, "International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)", Vol. 7, No. 2, 2021, https://doi.org/10.32628/CSEIT2172124
17. Mann, Monique; Matzner, Tobias, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, "Big Data & Society", Vol. 6, No.2, 2019, https://doi.org/10.1177/2053951719895805
18. Martins, Bruno, Oliveira; Jumbert, Maria, Gabrielsen, *EU Border technologies and the co-production of security 'problems' and 'solutions'*, "Journal of Ethnic and Migration Studies", Vol. 48, 2020, https://doi.org/10.1080/1369183X.2020.1851470

19. Martins, Bruno, Oliveira; Lidén, Kristoffer; Jumbert, Maria, Gabrielsen, *Border security and the digitalization of sovereignty: insights from EU borderwork*, "European Security", Vol. 31, No. 3, 2022, https://doi.org/10.1080/09662839.2022.2101884
20. Meden, Blaž; Rot, Peter; Terhörst, Philipp et al., *Privacy–Enhancing Face Biometrics: A Comprehensive Survey*, "IEEE Transactions on Information Forensics and Security", Vol. 16, 2021, https://ieeexplore.ieee.org/ielx7/10206/9151439/09481149.pdf
21. Orwat, Carsten, *Risks of Discrimination through the use of Algorithms, Federal Anti-Discrimination Agency*, Institute for Technology Assessment and Systems Analysis (ITAS), 2019, https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/EN/publikationen/Studie_en_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.pdf?__blob=publicationFile&v=2
22. Panchamia, Sanket, Byrappa; Deepak Kumar, Passport, *VISA and Immigration Management Using Blockchain*, "2017 23rd Annual International Conference in Advanced Computing and Communications (ADCOM)", 2017, https://doi.org/10.1109/ADCOM.2017.00009
23. Saunders, Natasha, *Security, digital border technologies, and immigration admissions: Challenges of and to non-discrimination, liberty and equality*, "European Journal of Political Theory", 2023, https://doi.org/10.1177/14748851231203912
24. Singaraj, S., Freddy, *Shroud of Surveillance and Its Threat to Fundamental Rights and Civil Liberties*, "Journal of Emerging Technologies and Innovative Research", 2019, https://www.jetir.org/papers/JETIRBH06007.pdf
25. Vavoula, Niovi, *The Transformation of Eurodac from an Asylum Tool into an Immigration Database*, "EU Immigration and Asylum Law and Policy", 2024, https://eumigrationlawblog.eu/the-transformation-of-eurodac-from-an-asylum-tool-into-an-immigration-database/
26. Wang, Yingxu; Tan, Xinming; Ngolah, Cyprian; Sheu, Philip; *The Formal Design Models of a Set of Abstract Data Types (ADTs),* "International Journal of Software Science and Computational Intelligence (IJSSCI)", Vol. 2, No. 4, 2010, https://doi.org/10.4018/jssci.2010100106

Documents

1. EU Monitor, *Annexes to COM(2020)779 - Functioning of the Schengen Evaluation and Monitoring Mechanism under Article 22 of Council Regulation (EU) No. 1053*, 2013, https://www.eumonitor.eu/9353000/1/j4nvirkkkr58fyw_j9vvik7m1c3gyxp/vle2l9lttgzy
2. European Commission, *EURODAC (European Asylum Dactyloscopy Database)*, 2022, https://knowledge4policy.ec.europa.eu/dataset/ds00008_en
3. European Commission, *Schengen Information System*, https://home-.affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en
4. European Commission, *Visa Information System (VIS)*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en
5. European Commission, *What is SIS and how does it work?*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en
6. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, *Security and Justice, Eurodac statistics*, https://data.europa.eu/data/datasets/eurodac-statistics?locale=en
7. European Union, Eurodac statistics, https://data.europa.eu/data/datasets/eurodac-statistics?locale=en
8. United States Government Accountability Office, *Biometric Identification Technologies Considerations to Address Information Gaps and Other Stakeholder Concerns*, Report to Congressional Committees, 2024, https://www.gao.gov/assets/gao-24-106293.pdf

Websites

1. https://data.europa.eu/
2. https://eumigrationlawblog.eu/
3. https://home-affairs.ec.europa.eu/
4. https://ieeexplore.ieee.org/
5. https://knowledge4policy.ec.europa.eu/

6. https://sciencespo.hal.science/
7. https://uclouvain.be/fr/
8. https://www.antidiskriminierungsstelle.de/
9. https://www.eumonitor.eu/
10. https://www.gao.gov/
11. https://www.jstor.org/

Iulia BULEA
Lucian Blaga University of Sibiu, Romania

HUMAN SECURITY IN THE CONTEXT OF MIGRATION AND THE ROLE OF INSTITUTIONAL COOPERATION IN CRIME PREVENTION

Abstract:	*Migration has become a pivotal global phenomenon, raising crucial concerns about human security and crime prevention. This article delves into the interconnectedness between human security and migration, emphasizing the importance of institutional cooperation in addressing these challenges. Human security, encompassing economic, social, political, and cultural dimensions, is a multi-faceted concept that becomes particularly relevant when discussing migration. Migrants often face vulnerabilities, such as exploitation, discrimination, and socio-economic instability, which can lead to heightened risks for both individuals and communities.* *A significant focus of the article is the role of institutional collaboration in enhancing human security and preventing crimes related to migration, such as human trafficking, smuggling, and organized crime. Government agencies, international organizations, and NGOs play a key role in managing these issues, ensuring that migration is handled in a way that minimizes risks while promoting safety and inclusion. Successful case studies of interagency collaboration highlight how information sharing, joint training, and coordinated intervention strategies have led to positive outcomes in safeguarding both migrants and local populations.* *However, the article also explores the challenges that hinder effective collaboration, such as resource constraints, conflicting interests, and coordination gaps. Restrictive migration policies can exacerbate these issues, making it more difficult for institutions to work together efficiently and placing additional strain on human security.* *To overcome these challenges, the article suggests strengthening institutional frameworks, fostering cross-agency communication platforms, and promoting education to raise awareness and reduce biases against migrants. A shift toward migration policies that prioritize human security is also recommended, aiming to protect both national interests and migrant rights, creating a safer, more inclusive environment for all involved.*
Keywords:	**Human security; public order; borders; migration; crime prevention; vulnerabilities.**
Contact details of the author:	E-mail: iulia.bulea@ulbsibiu.ro
Institutional affiliation of the author:	**Faculty of Law, Lucian Blaga University of Sibiu, Romania**
Institutions address:	Calea Dumbrăvii no 34, Sibiu, Romania, 550324, 0269233295, https://drept.ulbsibiu.ro/, drept@ulbsibiu.ro

Preliminary overview

In an increasingly interconnected world, the traditional understanding of security is expanding beyond the borders of nation-states. Today, human security has emerged as an essential area of study, emphasizing the safety and well-being of individuals as foundational to global endurance. This shift recognizes that issues such as migration, human rights, and social harmony are as significant as military defenses and international diplomacy. By focusing on human security, we can address the intricate challenges that migration brings, acknowledging its role in both strengthening and straining societies. It is surprising and intriguing that the concept of human security has only relatively recently come to the forefront of academic and policy discussions. For centuries, international bodies, governments, and leaders have used intricate strategies to

ensure the security of nation-states and sustain global peace. Yet, throughout the development of numerous theories, approaches, and perspectives in security studies, one element has often been neglected: the individual and their personal safety. The impact of migration on security is increasingly capturing the attention of researchers in fields such as political science, sociology, demography, economics, psychology, ecology, and military studies. The consensus views migration as a direct threat to national sovereignty and stability[1]. Yet, it is a phenomenon that cannot be eradicated. Solutions must be found to help all those involved adapt to the new conditions, to this new reality.

Migration, encompassing both emigration and immigration, impacts security through protective but also through destabilizing effects, influencing various dimensions, particularly psychological and social aspects. Globally, societies face a dual challenge: the loss of human resources in emigrants' home countries and concerns over potential disruption in host nations. Immigration brings forth issues like discrimination, marginalization, and labor exploitation, yet also enhances productivity and living standards. This dynamic is evident in the European Union, with Italy and Spain as prominent destinations and Bulgaria, Estonia, Latvia, and Romania as significant sources[2]. Governments are challenged to uphold fundamental human rights for all, including immigrants and citizens alike. Crafting effective policies requires balancing economic gains with social strength, aiming to integrate migrants while protecting the rights and welfare of everyone involved.

The interplay between migration and security is clear. On one side, migration often arises as a response to security threats that affect individuals, such as human rights abuses, ethnic tensions, or civil conflict. On the other side, if unmanaged, migration itself can lead to risks, fueling issues like organized crime and xenophobic violence. In Europe, both cases are visible: migration driven by insecurity was seen in the violent breakup of Yugoslavia, which created waves of refugees in neighboring countries, while migration as a source of insecurity was highlighted by the issues surrounding Romanian immigrants in Italy, Spain, and the United Kingdom in 2007. Migration can, however, also be viewed as a stabilizing force, a perspective this article will explore in further detail.[3] The varied impacts of migration require a setup that thoroughly considers each country's specific social and economic conditions. Developing policies that address these intricacies can help foster a more harmonious incorporation, strengthening both origin and host communities.

Furthermore, tragic incidents in places such as the USA, Spain, London, Beslan, India, Syria, and Ukraine, among others, indicate a potential link between migration, terrorism, and security. These events underscore a convoluted relationship, emphasizing the importance of a thorough analysis of migration's role within the larger framework of global security.[4] Examining the underlying causes and patterns of migration provide invaluable insights into how these movements interact with domestic and international security concerns. By tackling both the causes and effects of migration, policymakers develop strategies that reduce risks and encourage international collaboration and mutual support.

From personal safety to global stability

The layered interplay between migration and security calls for a nuanced approach, especially considering recent events that hint at deeper connections between migration patterns, terrorism, and national steadiness. These dynamics reveal how migration, far from being a single-layered phenomenon, is deeply woven into the fabric of human security. As communities manage the difficulties and benefits brought by migration, an equitable grasp of these matters is necessary. By adopting a human-centered path to security, nations can strengthen social harmony and work toward a safer world for everyone.

Migration offers numerous advantages, benefiting both destination and origin countries in unique ways. In host nations, migration helps address workforce gaps across various sectors, injecting new talent into fields like healthcare, technology, and agriculture. This workforce boost can stimulate economic growth, as migrants participate actively in the economy, both as employees and consumers, thereby generating increased demand for services and products. Culturally, migration introduces a rich diversity of perspectives, practices, and ideas, fostering a more dynamic and innovative social environment. In migrants' home countries, the financial support sent back plays an important role in improving family livelihoods, funding education, and supporting local businesses, which strengthens the local economy. Additionally, migrants often return with

[1] Valeriu Efremov, *Impactul migrației asupra situației de securitate*, "Moldoscopie", No. 2, 2017, p. 179
[2] Alexandra Sarcinschi, *Migrație și securitate*, Editura Universității Naționale de Apărare "Carol I", București, 2008, p. 4
[3] *Ibidem*, p. 5
[4] Valeriu Efremov, *Op. cit.*, p. 179

enhanced skills and insights from their experiences abroad, creating opportunities for knowledge transfer and development that benefit their communities.

Effective protection systems - whether at the national, regional, or global level - thrive only when each person feels safe and secure. Without this sense of personal safety, these structures become vulnerable, gradually weakening in their capacity. A threat to one individual can extend to their community and, by extension, to other connected groups whose equilibrium depends on the well-being of all members. Consequently, protecting individuals is a foundational imperative, given that human society operates as a system of interdependent components, each influencing the strength and equilibrium of the whole. This perspective highlights that individual protection forms the bedrock of a reliable system that genuinely meets citizens' needs. Ignoring protection at this level erodes public trust, creating soft spots that can weaken social and national coherence. Sustainable development of communities relies on policies that put citizen safety first, establishing a strong basis for a broader, durable defense system.

The concept of "security" is continually evolving, used to describe a wide range of concerns driven by diverse interests, which are presented—rightfully or not—as security priorities. Among academics and professionals, there is widespread agreement that security encompasses both territorial protection and the safeguarding of economic consistency, each seen as essential. These are viewed from two main perspectives: physical security - defense against external or internal threats—and the medium- and long-term survival of international actors, ensuring their continuity and balance. This expansive view of protection highlights a comprehensive procedure that goes beyond defense against immediate dangers, focusing also on long-term adaptability to future challenges. As a result, the concept broadens to integrate economic and social factors alongside traditional military aspects. Today, safeguarding societies includes handling cyber risks, climate change, and other evolving threats, requiring collaboration and continuous refinement of protective strategies.

National security implies a state of protection against external and internal dangers, maintained through dedicated measures to ensure a state's existence, independence, sovereignty, and territorial integrity, as well as respect for its concerns. It involves developing strategies and policies that safeguard values and guarantee long-term steadiness, with the goal of defending national interests and identity. Thus, national security transcends strictly military boundaries, integrating other dimensions such as economic and ecological aspects, which contribute to safeguarding and supporting the state's continuous development. This flexible model is a key in tackling today's range of issues, from digital security to environmental shifts, demanding coordinated efforts among countries and international partnerships. As cross-border and varied threats increase, governments must create unified security plans to ensure strong protection for all citizens affected by this phenomenon.

The concept of human security gained prominence only after the Cold War, as focus shifted from the exclusive defense of states to the protection and prosperity of individuals and communities. This method redefines safety as a matter of everyday welfare, addressing risks that impact daily life, such as economic instability, health crises, and environmental hazards. Practically, human security seeks to lessen deficiencies affecting both personal and societal lives, emphasizing the need to shield people from dangers. It encompasses a wider range of protective measures aimed at reducing various threats, including poverty, discrimination, and violence. By prioritizing individuals, this model bolsters equilibrium, fostering adaptable societies prepared to tackle a spectrum of obstacles in an increasingly connected world, where threats to one group can resonate more broadly. First presented in the United Nations Human Development Report (1994), the concept of human security has become central to modern international development perspectives, advocating for an angle that places human advancement and safeguarding fundamental rights at the forefront. This vision introduces a fresh model in politics, grounded in the responsibility of states to protect citizens and encourage growth, paving the way for a just and secure world where each person can thrive safely. By focusing on human needs, security evolves into a collaborative process among nations and organizations, establishing the groundwork for a more stable world. The integration of this concept worldwide marks a significant shift, recognizing individual protection as significant to lasting peace.

The relationship between migration, community endurance, and human security

In a rapidly globalizing world, societies are increasingly focused on securing pathways to prosperity at both public and individual levels. Migration, often sought for its economic and social opportunities, is widely seen as a practical strategy for personal and family advancement. However, this phenomenon also

brings forth nuanced hurdles, especially regarding the safety and quality of life of migrants and the families they leave behind. Today, efforts to enhance quality of life operate on multiple levels—from a broader scale, where countries and unions seek collective progress, to the more personal sphere, focusing on individual and family needs. In an interconnected world where resources and opportunities cross borders freely, migration remains a widely recognized path for improving living standards, shaped by economic and geopolitical forces. Some people alike idealize migration as a path to betterment and prosperity, envisioning new possibilities for economic security and personal growth. However, while migration can bring benefits, it also poses a significant obstacle to origin countries in the form of "brain-drain", where skilled individuals leave in search of opportunities abroad, potentially weakening the socioeconomic fabric of their home nations. This outflow of talent often leaves countries with shortages in some sectors, impacting local development and slowing progress. Yet, within the sphere of labor migration, human security emerges as a highly complex issue. This concept involves tackling both immediate threats, such as conflict or terrorism, and the longer-term, structural aspects necessary to ensure the safety and dignity of migrant workers and their families. Safeguarding migrant rights is fundamental, along with mitigating indirect social impacts, such as the emotional and social challenges faced by children left behind by migrating parents. Moreover, the creation of effective policies to protect migrants requires international collaboration to establish standards that extend beyond national borders, supporting migrants' security across various regions. Such policies must address physical safety and socio-economic steadiness, ensuring that migrant workers access fair employment, legal rights, and social services.

Today, the concept of identity is widely explored in specialized literature and appears in a range of contexts: cultural, national, ethnic, social, poetic, or collective. Here, our focus is on identity in the context of social changes experienced by migrants, particularly in relation to their interaction with the host society. The individual, as a social entity, generally retains core cultural and structural traits, as fundamental changes in contact with different societies would imply a transformation into a distinct social identity. To integrate, individuals often adopt and mimic certain behaviors—a process deeply rooted in social interaction.[1] At the same time, migration brings psychological and social pressures on families, especially children, who may experience its effects indirectly. Targeted initiatives are requisite to support families, alleviating isolation and fostering continuity within disrupted structures. Strengthening community support systems can promote consistency and encourage a nuanced perspective on migration—one that acknowledges economic benefits while prioritizing the overall comfort of individuals and families involved. An outlook on migration can ultimately cultivate a society flexible enough to adapt to change while ensuring that no one is left behind.

Migration has emerged as a key topic within human security discussions, acting as a force that shapes contemporary societies, and both reflects and drives massive transformations across diverse regions. As easy as people move across borders, migration represents more than a mere geographical shift; it prompts significant socio-cultural changes, reshaping the economic, social, and cultural landscapes of impacted communities. In both sending and host societies, migration initiates significant changes. Migration often brings about transformations in local communities as individuals leave behind family, social networks, and cultural connections. This departure can place pressure on traditional support systems, impacting families and communities that rely on migrants, especially for financial assistance. The influx of migrants calls for adaptations across social, economic, and political structures, influencing public policies, labor markets, and the provision of social services. The cross-border movement also has significant cultural implications for all involved, as migrants bring their cultural values, traditions, and practices, enriching the cultural fabric of host countries. This cultural exchange fosters understanding and tolerance, although managing cultural differences and potential tensions remains an important aspect of integration. Simultaneously, migrants often face the challenge of cultural adaptation, balancing the need to embrace the host culture with the desire to maintain their own cultural identity[2].

Labor migration reshapes economies by redistributing skills and resources across borders. In migrants' home countries, the financial support sent back not only sustains households but also stimulates small businesses and community projects, contributing to local economic growth. Meanwhile, in destination countries, migrant workers are indispensable to sustaining industries facing workforce shortages, such as

[1] Petronela Daniela Feraru, *Religie şi migraţie în România contemporană*, Lumen, Iaşi, 2016, pp. 200-201

[2] Viorica-Cristina Cormoş, *Migraţie şi identitate: Schimbări identitare, colective şi individuale, ca urmare a migraţiei internaţionale*, Editura Universităţii "Ştefan cel Mare", Suceava, 2011, p. 13

agriculture, healthcare, and construction, thereby fueling economic productivity and diversification. Nonetheless, alongside these benefits come challenges, including the need for policies that promote fair labor standards and protect migrant rights. From a security standpoint, migration brings questions of human safety and protection to the forefront. Migrants are vulnerable to exploitation, discrimination, and, at times, violence. Ensuring the human security of migrants involves implementing adapted policies that protect their rights and provide access to services like healthcare and legal assistance. For receiving communities, effectively managing migration flows involves balancing security considerations with humanitarian responsibilities to maintain public order. Here, migration can also impact political dynamics. Substantial migrant inflows can reshape public sentiment, steer political conversations, and affect electoral outcomes, as communities and policymakers adapt to the evolving needs and dynamics introduced by new population groups. These shifts often prompt a re-evaluation of social policies, resource allocation, and integration strategies, influencing national priorities and fostering dialogue on identity, inclusion, and economic impact. Through this process, both challenges and opportunities emerge, shaping the broader narrative around migration and its role in society. Policymakers must create setups that support migrant integration, fostering a sense of belonging while dealing with public concerns regarding security and resources. In areas affected by conflict or instability, migration serves as a survival strategy, allowing individuals to seek safety and opportunities in more developed regions. In such cases, human security becomes paramount, with migrants fleeing violence, persecution, or extreme poverty. This humanitarian aspect highlights the need for international cooperation and a shared responsibility in providing safe, legal migration channels.

Migration is also deeply connected to global inequality, with disparities in wealth, employment opportunities, and living standards often motivating individuals to seek better conditions for themselves and their families. Tackling these root causes calls for long-term solutions that reduce inequality and create opportunities within origin countries, making migration a choice rather than a necessity. At the same time, the environmental dimension of migration is becoming increasingly significant, as climate change compels people to leave regions impacted by natural disasters, rising sea levels, and resource depletion. This climate-driven migration introduces new human security challenges, requiring coordinated efforts to support displaced communities and help them rebuild their lives.

Romania's border police and the modern imperatives of migration management

The Romanian space has historically functioned as a borderland, consistently positioned at the periphery of large political and cultural realms. Throughout its past, it has marked the edge of significant empires and civilizations. For example, it once formed the frontier of the Roman Empire, dividing Roman influence from the "barbarian" territories, effectively cutting through what is now Romania, then known as Dacia. Similarly, it later stood at the limits of the Byzantine Empire, the Ottoman Empire, and served as the farthest reach of Western civilization. As the modern era unfolded, this area found itself precisely at the crossroads of three dominant empires, each exerting its influence: the Ottoman Empire, the Habsburg Monarchy, and the Russian Tsardom. Positioned on the outskirts of Russia, Germany, Austria, and Turkey, Romanians have often found themselves on the boundary of these powers. Today, this position persists, as Romania now sits on the edge of the European Union, serving as a frontier nation within its borders. This persistent "borderland" status has led to two distinct yet interconnected consequences. On one hand, it has fostered a certain degree of isolation, resulting in a slower adoption of external influences, the persistence of traditional structures, and a mindset deeply rooted in local values. On the other hand, this unique positioning has enabled an exceptional mix of ethnic and cultural influences converging from various directions, creating a vibrant mosaic of external and indigenous elements that define the region's character[1].

The unique position of Romania as a historical borderland has shaped both its identity and the responsibilities of its institutions, particularly those focused on national security and public safety. This borderland context has not only brought diverse cultural influences but has also underscored the importance of resilience and adaptability in response to shifting security pressures. In contemporary discussions, human security has become very important for managing and understanding these intricacies. focusing on safeguarding individuals and communities from threats that undermine their balance and quality of life. As a multidimensional component of human development, human security expands the focus beyond traditional

[1] Lucian Boia, *România, țară de frontieră a Europei*, Humanitas, București, 2012, p. 15

defense, incorporating both military and civilian dimensions and prioritizing responsive, coordinated action in times of crisis.

Personal security is a component of human development, positioned at its outer limits as it focuses on managing disruptions and institutional responses to such demands. This concept brings together both defense and civil sectors, establishing guidelines and plans for effective crisis response and management. The way institutions act in these contexts becomes emblematic of the general perception of them, directly influencing the trust and respect they receive from the public. Human security is closely tied to political legitimacy; we feel safe and trust our institutions when they demonstrate efficiency and responsibility in handling critical situations[1]. Furthermore, human security involves the capacity to foresee and counteract threats that could undermine social harmony and the overall quality of community life. By adopting proactive measures, institutions reduce vulnerabilities and create a safe social climate for citizens. Additionally, the implementation of transparent policies and the active involvement of civil society in security processes strengthen the relationship between authorities and citizens. Within this blueprint, the Romanian Border Police, as part of the Ministry of Internal Affairs, serves as a key factor in monitoring and controlling state borders, with a significant focus on preventing and combating illegal migration and cross-border criminal activities. This body collaborates with other national institutions responsible for law enforcement and public order, ensuring integrated efforts to safeguard borders and uphold national security. Romanian Border Police responsibilities extend to maintaining lawful border crossing procedures, ensuring the safety of persons and assets, and preventing potential migration-related security risks.

In fulfilling its duties, the Romanian Border Police utilizes a comprehensive database that facilitates efficient monitoring and record-keeping. It includes data on individuals, transportation means, goods, and instances of interdiction or flagged items at border crossings, all aimed at preventing unauthorized entry or exit. Moreover, it aids in tracking cases of document forgery, suspicious individuals, and goods subject to restrictions, creating a structured mechanism for oversight in both national and international contexts. The Romanian Border Police engages actively in partnerships with global law enforcement bodies and institutions, building alliances to strengthen border security measures and enhance collective response efforts. Collaborating closely with entities like INTERPOL, Europol, and Frontex, they work to counter transnational threats and uphold regional endurance. These partnerships are essential in organizing joint operations, sharing intelligence, and coordinating activities at the external boundaries of the EU. Within the framework of Frontex, the Romanian Border Police contributes personnel and technical resources to joint efforts, emphasizing the importance of integrated tactics to address migration and border-related security issues. At a broader level, the Romanian Border Police also collaborates with local authorities and port administrations to ensure that all border activities are conducted within legal guidelines. These collaborative efforts are designed to ensure secure and regulated migration processes, combat human trafficking, and tackle the challenges associated with illegal migration and transnational crime. This collaboration underscores the need for a unified strategy, integrating efforts from both national agencies and international bodies to uphold human security standards and address migration-associated risks comprehensively[2].

The European Union has developed a unified strategy for managing migration through Frontex, an agency that assists European Union member countries and Schengen affiliates in securing the EU's outer borders and tackling transnational crime. In close cooperation with national authorities, EU bodies like Europol, and international organizations, Frontex enhances security across the European Union by actively confronting transnational criminal activities. The agency's operations extend beyond countering migrant smuggling and human trafficking, targeting a range of serious crimes that endanger EU security, such as drug and arms trafficking, vehicle theft, counterfeiting, document forgery, and ecological breaches. Numerous criminal networks expand their unlawful operations by incorporating migrant smuggling or human trafficking, often using the same routes and tactics for moving other illicit goods. These networks frequently collaborate across various forms of organized crime, supporting activities such as the production of fake documents, arms distribution, corruption, and money laundering.

[1] Mary Kaldor, *Securitatea umană: reflecţii asupra globalizării şi intervenţiei*, CA Publishing, Cluj-Napoca, 2010, p. 216

[2] *Ordonanţa de Urgenţă a Guvernului nr. 104/2001 privind organizarea şi funcţionarea Poliţiei de Frontieră Române*, https://legislatie.just.ro/Public/DetaliiDocument/29274 (3.12.2024)

The nature of cross-border crime calls for a coordinated and proactive method at the EU's borders, which serves as a vital line of defense to intercept threats before they impact EU citizens and disrupt internal stability. To effectively counter these challenges, Frontex, together with EU member states and non-EU partners, shapes its border operations around detailed risk assessments and crime trend analyses. The agency provides technical and operational support to EU Member States, including expertise, specialized training, advice on advanced technological tools, and the capacity to initiate direct operational actions. Law enforcement plays a central role in Frontex's missions, with every joint operation designed to counteract cross-border crime. Frontex also participates in Joint Action Days, international initiatives that unite national law enforcement, global organizations, and EU entities under the EMPACT (European Multidisciplinary Platform Against Criminal Threats) to tackle organized crime through coordinated efforts. Through aligning its crime prevention measures with assistance from European and international partners, Frontex fosters a unified path to security, strengthening the EU's external borders and bolstering resilience against criminal threats[1].

Europe stands as a central hub for international migration, experiencing flows not only within its own borders but also from other continents. Despite shifts in the boundaries of the European Union through the inclusion of new members, the notion of international migration remains pertinent for individuals who cross national borders to establish residence or join the labor force in a new area. This classification holds true even for EU citizens, such as those from Romania or Bulgaria, who meet these migration criteria and are thus still regarded as immigrants despite their countries' EU membership. The continued relevance of national borders within the Union underscores that, rather than simply internal mobility, such movement is still identified as international migration within the EU context. This distinction reflects the complexity of migration in Europe, where economic, social, and legal dynamics shape a diverse migration landscape that requires careful policy consideration to manage both integration and border security effectively[2].

Institutional strategies and cross-border collaboration during the Ukrainian crisis

Building on Romania's historical borderland legacy, the institutional frameworks and strategic collaborations exemplify the evolving role of national and transnational entities in managing migration challenges. As the narrative transitions from Romania's border management to its broader implications during crises such as the Ukrainian conflict, the importance of a unified European response becomes increasingly evident. This shift in focus highlights the interplay between localized institutional efforts and broader EU strategies, emphasizing both the challenges and the opportunities presented by cross-border cooperation. The war in Ukraine, sparked by Russia's invasion, has led to one of the largest refugee crises in Europe since World War II. Millions of Ukrainians have fled their homes, seeking refuge primarily in EU member states such as Romania, Poland, Germany, and Hungary. This massive displacement has put the European Union's migration management systems to the test, highlighting both strengths and weaknesses in its frameworks while showcasing the critical importance of cooperative security strategies like the Strategic Compass for Security and Defence. Alongside migration management, the crisis has also intensified efforts to prevent and combat transnational crimes, which are often exacerbated during mass migration movements.

The Ukrainian crisis unfolded at a rapid pace, requiring an equally swift response. Unlike previous migration challenges, the EU demonstrated a strong sense of solidarity and unity. The Temporary Protection Directive was activated for the first time, granting displaced Ukrainians immediate access to residency, employment, healthcare, and education across member states without the need for lengthy asylum procedures. At the same time, significant humanitarian aid was mobilized to support both refugees and the neighboring countries most affected by the crisis. These measures underscored a shift in the EU's approach to migration, one that prioritized human security principles while maintaining border management and societal stability. Preventing and combating transnational crimes such as human trafficking, smuggling, and organized crime networks became an essential component of the EU's response. Agencies like Europol, Eurojust, and Frontex played pivotal roles in ensuring that security threats did not escalate as migration flows increased. Europol, the EU's law enforcement agency, worked closely with national police forces to identify and dismantle smuggling rings exploiting vulnerable refugees. Operation Sentinel, coordinated by Europol, targeted networks involved

[1] Frontex, *Fighting crime. Tackling cross-border crime*, https://www.frontex.europa.eu/what-we-do/fighting-crime/cross-border-crime/ (3.12.2024)
[2] Alexandra Sarcinschi, *Op. cit.*, p. 30

in smuggling Ukrainians across EU borders illegally[1]. Eurojust, the EU's judicial cooperation agency, supported investigations by facilitating cross-border collaboration among prosecutors, ensuring that criminal groups could not exploit jurisdictional gaps[2].

Frontex, the European Border and Coast Guard Agency was instrumental in reinforcing border controls while upholding human security standards. The agency deployed additional personnel to external EU borders, conducted risk analyses, and monitored migration routes to prevent exploitation by criminal networks[3]. Simultaneously, Frontex ensured compliance with EU laws protecting refugees, emphasizing humane treatment and safeguarding rights. In parallel, the European Union Agency for Law Enforcement Training (CEPOL) provided specialized training programs to law enforcement officers, equipping them with skills to detect and respond to human trafficking and other crimes associated with migration crises[4]. The Strategic Compass, adopted during the early days of the Ukrainian crisis, provided a guiding framework for these efforts. Although primarily a defense and security strategy, the Compass includes provisions that directly address challenges related to migration, human security, and transnational crime. It emphasizes the importance of resilience and crisis preparedness, recognizing the need for a coordinated approach to hybrid threats such as mass displacement and the criminal activities it often triggers[5]. The crisis demonstrated the value of pre-existing legal frameworks and contingency plans, which allowed the EU to respond decisively and avoid some of the missteps of previous migration crises. The Strategic Compass also reflects a delicate balance between border security and humanitarian obligations. While reinforcing the role of agencies like Frontex in managing external borders, it integrates human security considerations to ensure that those fleeing conflict are protected. The Strategic Compass emphasizes the EU's commitment to a "more capable and resilient Union" by enhancing collective security measures and fostering operational readiness among member states. This vision reflects a deliberate effort to balance border security with the protection of fundamental rights, aligning with the broader objectives of human security principles[6] The seamless activation of the Temporary Protection Directive and the pooling of resources among member states highlighted the benefits of enhanced coordination, a principle central to the Compass. According to the Temporary Protection Directive, member states are required to ensure immediate access to protection mechanisms and essential services for those fleeing mass displacement events, reinforcing the need for coordinated and standardized responses to migration crises[7]. However, the crisis also exposed certain limitations. Border countries like Romania and Poland faced overwhelming pressure as first points of entry, while disparities in national capacities and infrastructure created bottlenecks in the distribution of refugees across the EU. Although solidarity mechanisms were in place, the uneven burden-sharing underscored the need for more robust and permanent structures to address such crises effectively.

Human security emerged as the cornerstone of the EU's response. Unlike traditional state-centric approaches to migration, which prioritize border control and sovereignty, human security focuses on the protection of individuals and their well-being. The activation of the Temporary Protection Directive demonstrated the EU's ability to swiftly provide temporary refuge for displaced persons during times of crisis, showcasing its commitment to solidarity and shared responsibility among member states. However, disparities in national capacities highlighted the challenges of implementing such measures equitably across the Union.[8] The immediate granting of safeguard under the Temporary Protection Directive offered displaced Ukrainians stability and hope, while integration programs in host countries addressed essential needs such as language training, access to education, and vocational opportunities. This approach not only safeguarded the dignity of refugees but also strengthened social cohesion in host communities.

Despite these successes, the Ukrainian crisis has also drawn attention to challenges that the EU must address. The preferential treatment afforded to Ukrainian refugees compared to those from other regions, such

[1] Alexandra Sarcinschi, *Op. cit*., p. 78
[2] European Commission, *Eurojust Annual Report 2022*, Brussels, 2023, p. 34
[3] Frontex, *Risk Analysis for 2022*, Warsaw, 2022, p. 12
[4] CEPOL, *Annual Activity Report 2022*, Budapest, 2023, p. 24
[5] European External Action Service, *A Strategic Compass for Security and Defence*, Brussels, 2022, p. 8
[6] *Ibidem*, p. 45
[7] Council of the European Union, *Temporary Protection if There is a Mass Influx of Displaced People*, Brussels, 2022
[8] European Parliament, *Temporary Protection Directive*, Brussels, 2022, p. 9

as the Middle East or Africa, raised concerns about the consistency of the EU's commitment to human security principles. Critics have pointed to the need for more equitable policies that avoid perceptions of selective compassion and ensure fair treatment for all migrants, regardless of their origins. Furthermore, transnational crime networks remain a persistent threat, requiring sustained cooperation between international organizations, national law enforcement, and NGOs to mitigate risks and protect the most vulnerable. Organizations like the International Organization for Migration (IOM) and the United Nations Office on Drugs and Crime (UNODC) have been crucial in supporting EU efforts to prevent and combat transnational crime during the Ukrainian crisis. The IOM provided data and expertise on migration flows, helping to identify trafficking trends and improve protection mechanisms for refugees. The UNODC worked alongside the EU to strengthen border management systems and combat organized crime through capacity-building programs and technical assistance. These collaborations demonstrate the importance of a multilayered approach to security, where international, regional, and local actors work in tandem.

Looking ahead, the lessons learned from the Ukrainian crisis offer a pathway for improving the EU's migration management systems. The Strategic Compass provides a valuable roadmap, but its objectives must be operationalized through concrete policies with clear benchmarks. Greater investment in capacity-building for border states and the creation of a permanent solidarity mechanism could alleviate the disproportionate pressure on certain countries. Enhanced collaboration with organizations like Europol, UNODC, and the IOM is essential to addressing both the immediate and long-term challenges of displacement. The Ukrainian crisis has underscored the interconnectedness of migration, security, and human dignity. By fully embracing the principles outlined in the Strategic Compass and reinforcing the importance of preparedness, cooperation, and human security, the EU has an opportunity to establish itself as a global leader in migration management. This crisis has not only tested its resolve but has also provided a blueprint for addressing future challenges with compassion, resilience, and unity, while preventing transnational crime from undermining its efforts.

Final considerations

As a leading example of regional integration, the European Union preserves national borders while introducing the concept of European citizenship beyond them, simultaneously applying Schengen Area rules for some member states[1]. However, despite significant progress, managing migration effectively requires overcoming persistent challenges.Institutional collaboration faces barriers such as limited resources, varied policy priorities, and coordination issues. Diverging national procedures to migration can create friction; some countries emphasize border security to control migration, while others focus on migrant integration and rights protection. This divergence can hinder collaborative effectiveness. Additionally, restrictive migration policies can increase migrant vulnerability, as seen in cases where stringent immigration laws have inadvertently fostered exploitative practices. For instance, strict border policies can make migrants more susceptible to trafficking and smuggling networks. Responding to these challenges requires robust institutional outlines and streamlined communication between agencies involved in migration management. Initiatives such as interagency task forces facilitate joint efforts, resource sharing, and coordinated responses to migration-related security concerns. The United Kingdom's Modern Slavery Taskforce is a prominent example of such collaboration, bringing together diverse law enforcement bodies to address trafficking and exploitation with notable success in victim identification and prosecution efforts.

Education and training are also integral to fostering an informed and culturally aware workforce. Programs like those offered by the European Police College (CEPOL) equip officials with critical skills in areas such as migrant rights and crisis response, promoting fair and humane treatment of migrants while strengthening operational preparedness. A shift toward migration policies rooted in human security principles is imperative to building a safer environment for migrants and local communities alike. Policies that balance humanitarian values with security objectives can help reduce migrant vulnerabilities while supporting social unity. Canada's immigration model, which emphasizes legal pathways, work opportunities, and refugee protection, has proven effective in minimizing migrant risks while meeting labor demands and facilitating integration In Europe, the New Pact on Migration and Asylum, introduced by the European Commission in

[1] Alexandra Sarcinschi, *Migraţia ca problemă de securitate*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2014, p. 6

2020, reflects an evolving commitment to a fair and cooperative migration system. By proposing streamlined asylum processes, enhanced border management, and greater solidarity among member states, the pact aims to establish a sustainable migration management system. This renewed commitment positions the EU to address migration-related challenges comprehensively while upholding human rights and promoting security across the region.

Bibliography

Books

1. Boia, Lucian, *România, ţară de frontieră a Europei*, Humanitas, Bucureşti, 2012
2. Cormoş, Viorica, Cristina, *Migraţie şi Identitate: Schimbări identitare, colective şi individuale, ca urmare a migraţiei internaţionale*, Editura Universităţii "Ştefan cel Mare", Suceava, 2011
3. Feraru, Petronela, Daniela, *Costuri sociale ale migraţiei externe din România*, Editura Lumen, Iaşi, 2019
4. Feraru, Petronela, Daniela, *Religie şi migraţie în România contemporană*, Lumen, Iaşi, 2016
5. Kaldor, Mary, *Securitatea umană: reflecţii asupra globalizării şi intervenţiei*, CA Publishing, Cluj-Napoca, 2010
6. Micu, Gabriel, *Ordinea juridică instituţională comunitară*, Paideia, Bucureşti, 2007
7. Neag, Mihai, Marcel, *Securitatea umană în conflictele şi crizele internaţionale*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2010
8. Neag, Mihai, Marcel, *Garantarea securităţii umane*, Volumul I – Rolul instituţiilor de securitate şi al societăţii civile, Editura Sitech, Craiova, 2010
9. Neag, Mihai, Marcel, *Garantarea securităţii umane*. *Securitatea umană prin integrare europeană şi dezvoltare umană*, Vol. II, Editura Sitech, Craiova, 2010
10. Răducu, Cătălina, Daniela; Ştefanachi, Bogdan, *Securitatea umană. Provocări contemporane,* Editura Pro Universitaria, Bucureşti, 2015
11. Sarcinschi, Alexandra, *Migraţia ca problemă de securitate*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2014
12. Sarcinschi, Alexandra, *Migraţie şi securitate*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2008

Article

1. Efremov, Valeriu, *Impactul migrației asupra situației de securitate*, "Moldoscopie", No. 2, 2017

Documents

1. Council of the European Union, *Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof, Official Journal of the European Communities, L 212,* Brussels, 2001
2. Council of the European Union, *Temporary Protection if There is a Mass Influx of Displaced People,* Brussels, 2022
3. European Parliament, *Temporary Protection Directive,* Brussels, 2022
4. European Commission, *Eurojust Annual Report 2022,* Brussels, 2023
5. European External Action Service (EEAS), *A Strategic Compass for Security and Defence,* Brussels, 2022
6. European External Action Service, *A Strategic Compass for Security and Defence,* Brussels, 2022
7. Frontex, *Risk Analysis for 2022,* Warsaw, 2022
8. CEPOL, *Annual Activity Report 2022,* Budapest, 2023

Websites

1. https://www.consilium.europa.eu/
2. https://www.frontex.europa.eu/

Juliana GJINKO
University of Tirana, Albania

FROM CRISIS TO COHESION. EXAMINING THREE DECADES OF ALBANIAN MIGRATION AND INTEGRATION IN ITALY

Abstract:	*The mass emigration of 1991, the mass migration following the 1997 financial crisis, and the migrant surge during the Kosovo conflict in 1999 were the three main waves of Albanian migration to Italy. In addition to the initial surprise and lack of preparation on the side of the Italian people and governmental bodies, each of these waves was marked by incredibly challenging initial conditions. The Albanian immigrants' integration process is today viewed as a largely successful narrative. What were the primary causes of the comparatively quick integration following such a dramatic beginning? Young age, medium educational attainment, big family size, lack of religious affiliation, and comparatively high level of familiarity with Italian language and popular culture are characteristics that identify Albanian immigrants. Also, the Italian government has taken significant steps towards integration, including legalizing undocumented immigrants and reaching agreements with their Albanian counterparts on the repatriation of Albanian individuals convicted of crimes.* *The primary issues and patterns that have surfaced during three decades of migrant flows are examined in this article. Particularly, it emphasizes integration into the workforce and culture, and how the media depicts and influences the relationship between migrants and the host country. Integration data have been examined in the context of Italian political and social dynamics. A few integration factors have also been studied, with a focus on the demographics of migrants and refugees during the main migratory waves. It may be possible to determine the least stressful and most successful cohabitation techniques throughout Europe's difficult and ongoing migrant waves by looking at these integrating components.*
Keywords:	**Migratory flows; challenges; integration; workforce; education**
Contact details of the authors:	E-mail: juliana.marko@unitir.edu.al
Institutional affiliation of the authors:	**University of Tirana, Albania**
Institutions address:	Rr. Elbasanit, Tiranë, Tel.: +3554 22369987E -mail: fhf@fhf.edu.al Website: fhf.edu.al

Introduction

Migration has had a long and complex relationship with Albania and its people. For centuries, Albanians have moved throughout the world, looking for better economic opportunities. In certain periods, such as the mass emigration from the late 19th century through the end of the Second World War, the number of Albanian migrants constituted a sizeable portion of the population. Between 1990 and 2020, migration has been used by a significant number of Albanians to escape economic hardship and lack of opportunity created by the breakdown of centralized state planning. These economic and social conditions resulted in widespread poverty and unemployment, social tension and upheaval, resulting in political turmoil and ethnic violence. Despite a period of high economic growth from 2000 to 2008, the disparity with Western Europe starkly demonstrates the unfinished transition to a stable, high-income, modern, and equitable society.

The striking fact is that Albanian migration to Italy presents three main waves clearly denoted by the changing legal and economic aspects at play. The first wave in the early 1990^{s}, composed mostly of economic

migrants, was of the clandestine type, framed by the collapse of a centralized economic model and a migration regime characterized by the absence of a treaty, permissive national policy, and only informal presence of the state in the migration system. The shift towards an orchestrated system of migration recognized by migration regime legalities started three years later in 1993. Indeed, the second wave began in 1994 when a treaty aiming for the legalization of irregular migrants from Eastern Europe, such as ethnic Albanians who fled since August 1991, constantly meeting this requirement and having used the spring mass migration route towards Italy, came into force[1]. This marked a turning point in the Albanian migration to Italy, as it allowed for a more regulated and structured approach. The effects of this treaty were further solidified by a series of regularization ordinances in 1995 and 1998 that legalized immigrants who had worked with a regular residence permit for at least three years, providing them with a sense of stability. Finally, in response to the increasing number of migrants and the need for better management, a law aimed at regulating labor forms and migration quotas was introduced, establishing guidelines and limitations for the labor force and immigration flow. This comprehensive approach aimed to address the economic and social impacts of migration while ensuring a more controlled and structured system[2].

A sought-after, more desirable and highly coveted feature of residence permits, combined with the process of legalized migration, has significantly diminished the geographical distances between countries as air travel became more accessible. This development has remarkably facilitated family reunification, especially for vulnerable groups such as women and minors who were left behind in their countries of origin. These individuals, now armed with affordable and rapid means of transportation, were able to embark on the journey to their host countries. This profound shift in migration patterns may potentially account for the increasing number of individuals returning to their country of origin as well as the parallel decrease in circulation among Albanian migrants and returnees from 1995 until the eve of the second Albanian crisis, which was officially declared in 1997. During this period, approximately 150,000 asylum seekers took a courageous stance and migrated in search of what they perceived to be a beacon of democracy and shared development standards.

As a result, there was a noticeable surge in their population within the host country. Alongside this influx, Italy experienced a significant increase in the construction labor market. The number of working hours rose by an estimated 200,000,000, which translates to roughly 124,000 additional employees between 1998 and 2004. This wave of migration was predominantly driven by the desire for family reunification, with numerous first-generation linkages occurring through marriages between Italian citizens and immigrants[3]. Subsequently, marriages between immigrants themselves became increasingly common. Additionally, the frequent occurrence of clause laws for reunification with ascendants or dependents further contributed to this family-oriented wave of migration. It is worth noting that although the percentage of female resident workers is stabilizing at around 33%, it remains lower than that of foreign resident workers. In fact, foreign resident workers make up approximately 50.6% of the population[4].

The dynamics of migration shifted once again in 2000-2001 when the United Nations administration, supported by the Italian government and endorsed by the Security Council, successfully restored administrative and public institutions in Kosovo[5]. This led to a voluntary return of immigrants with Serbian and Albanian Kosovar origins due to both economic and political reasons. Consequently, the number of immigrants from this region decreased significantly. The third wave of migration, which can be characterized by both semi-clandestine and legally formalized migration, introduced new dimensions to the phenomenon. This wave utilized the concept of international protection as a pretext for reception. Many individuals sought political asylum, which often resulted in pending requests. The porous nature of borders and territories, compounded with the prevalence of illegal identifications, facilitated the continuous flow of immigrants while evading strict controls. This phenomenon enabled anonymity and allowed individuals to escape detection

[1] King Vullnetari, *Migration and Development in Albania*, Sussex Centre for Migration Research, Sussex December 2003, p. 25, https://eprints.soton.ac.uk/377327/1/WP-C5.pdf (12.11.2024)

[2] Eda Gemi, Anna Triandafyllidou, *Rethinking migration and return in Southeastern Europe: Albanian mobilities to and from Italy and Greece*, Routledge, London, 2021, p. 6

[3] Barjaba King, *Introducing and Theorising Albanian Migration*, "The New Albanian Migration", edited by Russell King, Nicola Mai & Stephanie Schwandner-Sievers, Sussex Academic Press, Brighton, 2005, p.15

[4] Pittau Ricci Urso, *Gli Albanesi in Italia: un caso di best practice di integrazione e sviluppo*, "REMHU: migracoes e desenvolvimento", Vol. 17, No. 33, 2009, p.77

[5] *Ibidem*, p.155

while perpetuating smuggling activities. The absence of comprehensive policies on legal family formation and regularization, like those implemented in other European countries, further exacerbates this issue. Under the prevailing search privileges regime, emergency hospitality takes the form of temporary accommodation as a response to asylum applications made within the country.

This approach is directly proportional to the volume of asylum requests. Furthermore, taking a customizable route from the neighboring Balkan countries towards the shores of Italy has introduced new challenges. This route often involves the reception of forced mothers who are trafficked with minors, both of whom are subjected to affirmative or penal instances against their accomplices. Over the course of 30 years, this migration route has witnessed the arrival of over 600,000 individuals, solidifying their position as the second largest foreign community in Italy—a testament to the enduring allure of this European heartland[1].

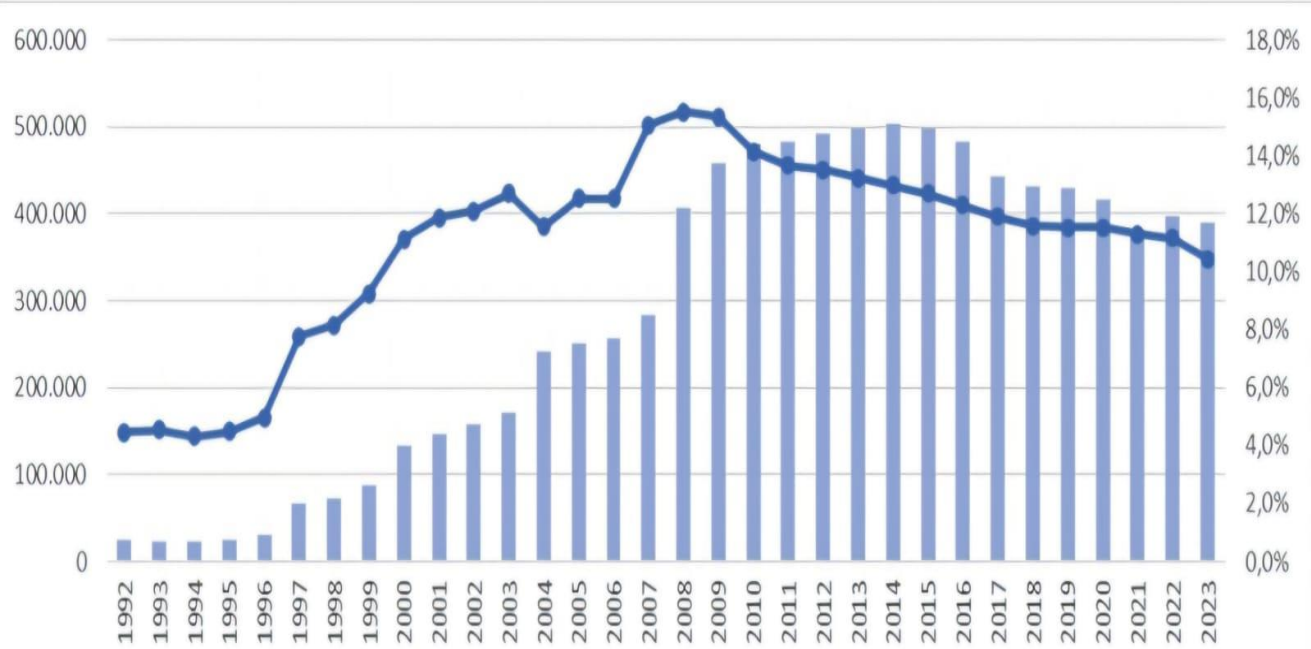

Table 1. Albanian citizens regularly residing and incidence on the total number of regularly residing, 1992-2023[2]

The socio-economic impact of the mass migration of the last two decades has become an interesting and highly debated issue in academic circles and research. Numerous works have extensively examined the diverse and intricate structural effects of Albanian immigration. However, only a few have delved into the direct microeconomic equilibrium effects on the communities from which the migrants originate. The decades-long wave of mass emigration has given rise to a notable phenomenon known as the 'dual economy' in Albania[3]. Throughout this period, it is worth noting that the participation of the diaspora in the social and economic development of the country has been severely limited, resulting in relatively minimal fundamental changes to the existing socio-economic landscape. When reflecting on the destination country, Italy, one can observe that various significant diachronic moments have shaped the trajectory of the Albanian community's interaction within it. Initially, the community predominantly engaged in housework, forming an essential backbone of domestic labor. Subsequently, their roles shifted towards unqualified work or involvement in off-

[1]Ministero del Lavoro e delle Politiche Sociali, *Rapporto Comunità albanese in Italia. Rapporto Annuale dulla Presenza dei Migranti*, Roma, 2023, p. 2

[2] Ministero del Lavoro e delle Politiche Sociali, *Rapporto Comunità albanese in Italia. Rapporto Annuale dulla Presenza dei Migranti*, Roma, 2023, p. 8 https://www.lavoro.gov.it/sites/default/files/temi-e-priorita%2C%20immigrazione/studi-e-statistiche/RC_Albania_2023_def.pdf (03.05.2024)

[3] Sabatino Bonifazzi, *Albanian migration to Italy: what official data and survey results can reveal*, "Journal of Ethnic and Migration Studies", Vol. 29, No. 6, p. 970, https://www.tandfonline.com/doi/abs/10.1080/1369183032000171320 (22.09.2024)

ethnic businesses. Despite these adaptations, the Albanian community has consistently remained on the margins of the collective life of the host society, without fully integrating or benefiting from their contributions.

The situation of unpreparedness regarding migratory flows has been addressed in three phases, through three important laws: in 1990, urgent provisions on political asylum, entry and residence of non-EU citizens and regularization of non-EU citizens and stateless persons present in the territory of the State (Legge Martelli)[1]; in 1998, a consolidated law on immigration and the condition of foreigners (Legge Turco-Napolitano)[2], and in 2002 numerous amendments modified thee 1990 Law adding regulatory provisions (Legge Bossi-Fini)[3]. This consolidated body of laws intervened in the main areas of immigration: immigration law in the strict sense, concerning the management of the migratory phenomenon as a whole: the definition of rules for entry, residence, control, stabilization of migrants and also the repression of violations of these rules; and integration law, which concerns the extension, to a greater or lesser extent, of the rights of citizens (civil, social, political rights) to migrants. The fundamental underlying principles were essentially three: the planning of migratory flows and the fight against illegal immigration (regarding immigration law); the granting of a wide range of rights aimed at the integration of regular foreigners (integration law).

The many socio-economic advantages for traditional community functions recognized in various states, especially in Germany, where, for example, Albanians benefit from facilitated taxable capital repatriation and many other significant benefits, also stimulate new investments and the deployment of pressure on the management and enhancement of uncontrolled remittances sent by migrants from Germany to Albania[4]. In Italy, we note the fair number of remittances sent, particularly in family integration plans, which are much lower compared to Germany. This is partly due to the constant political management of the immigrant phenomenon, which has practically transformed these flows into a consistent protection of national funds by Albania, which continues today, even if competition has gradually reduced the monetary demand made by Italians of Albanian origin for products made in Italy.

Additionally, it is important to highlight that the integration policies implemented by Germany have been instrumental in attracting many Albanian immigrants, who have found numerous opportunities for social and economic advancement in the country[5]. These policies have not only facilitated the entry and stay of Albanians in Germany but have also provided them with access to various social welfare programs, educational opportunities, and employment prospects. As a result, many Albanians in Germany have been able to establish stable lives, contribute to the local economy, and maintain strong ties with their home country. Moreover, the favorable taxation system in Germany has further incentivized Albanian entrepreneurs and investors to seize business opportunities, leading to an increase in trade and economic cooperation between the two nations. Overall, the integration of Italians of Albanian origin has varied across different countries, with Germany emerging as a particularly attractive destination for migrants due to its comprehensive support structures and economic incentives.

During the past years of exceptional Albanian emigration, the reports and studies concerning them and their future were incredibly dismal, to say the least. As of today, Italy possesses not only 30 years of experience with this migrating population, but also a notable number of second-generation descendants who

[1] *Gazzetta Ufficiale n.49 del 28 Febbraio 1990,* https://www.gazzettaufficiale.it/gazzetta/serie_generale/caricaDettaglio?dataPubblicazioneGazzetta=1990-02-28&numeroGazzetta=49 (21.04.2024)

[2] *Gazzetta Ufficiale n. 59, Supplemento Ordinario n. 40 del 12 marzo 1998*, https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1998-03-12&atto.codiceRedazionale=098G0066&elenco30giorni=false (22.04.2024)

[3] *Gazzetta Ufficiale n. 199 del 26 Agosto 2002*, https://www.gazzettaufficiale.it/eli/gu/2002/08/26/199/sg/pdf (21.04.2024)

[4] Mai Russell, *Out of Albania. From Crisis Migration to Social Inclusion in Italy*, Bergahn Books, Brooklyn NY 2008, p.121

[5] Begotaraj Ngjela, *Population movements and migration as a trend: the case of Albania*, "Journal of Balkan Studies", Vol. 2, No. 1, 2022, pp. 65-81

appear to have firmly established themselves in the local society[1]. The implementation of various regularization and supportive laws has significantly contributed to shedding a less tragic light on this situation.

Reason of the permit	V %	Variation % 2021/2020	Incidence on total non EU citizens (%)
Work	20,3%	559,3%	11,8%
Family	59,0%	106,5%	14,2%
Study	1,5%	132,8%	2,5%
Asylum and other forms of protection	1,1%	98,2%	98,2%
Elective residence, religion, health	18.0%	52.8%	27.7%
TOTAL – 29.520	100%	124.0%	12.2%

Table 2. - New residence permits issued to Albanian citizens in 2021 by reason and citizenship. V.% and variation 2021/2020[2]

The most significant indication of progress regarding the standing of these immigrants is the fact that now, in the second decade of the 2000s, migrants are frequently opting to return to Albania voluntarily. These returns are motivated either by the desire to fulfill personal and professional projects that have further developed in their new country of residence, or because of professional downsizing and unemployment resulting from recent crises, such as the economic downturn in Italy and Europe[3]. These returnees have vastly contributed to establishing flourishing businesses in their homeland. They achieve this by not only transferring the technologies and production methodologies they acquired in Italy, but more importantly, by importing goods and supplies from Italy, which are produced in large volumes at competitive costs. The heightened integration of recent and future generations of migrants, combined with the experience and financial capabilities of their predecessors, renders these migration processes genuinely virtuous and beneficial not only for the economic advancement of the migrants themselves, but also for the overall societal structure of Albania.

In the Italian context, the media tends to extensively showcase news that primarily focuses on portraying Albanians in a negative light. This is done by placing strong emphasis on criminal activities or highlighting their challenging living conditions within the host country. It is crucial to acknowledge that the media holds great influence as a catalyst in society, as it has the power to polarize communities and position them in relation to one another. Furthermore, it possesses the ability to bring about transformative effects by not only providing information but also by constructing reality through various representations. When it comes to the formation of national identity, the media plays a highly influential role by determining what is deemed newsworthy. This is particularly significant, as it involves the media's decision-making process on which topics to cover, how to cover them, and ultimately impacting the way in which the national "other" is portrayed with the intention of either worsening or improving such representations[4].

[1] Zana Vathi, *The children of Albanian migrants in Europe: ethnic identity, transnational ties and pathways of integration*, University of Sussex, 2011, p. 35, https://sussex.figshare.com/articles/thesis/The_children_of_Albanian_migrants_in_Europe_ethnic_identity_transnational_ties_and_pathways_of_integration/23316749?file=41104385 (21.09.2024)

[2] Ministero del Lavoro e delle Politiche Sociali, *Rapporto Comunità albanese in Italia. Rapporto Annuale dulla Presenza dei Migranti,* 2022, p.10, https://www.lavoro.gov.it/sites/default/files/documenti-e-norme/studi-e-statistiche/RC-Albania-2022.pdf (23.05.2024)

[3] Cristiana Paladini, *Circular migration and new forms of citizenship. The Albanian community's redefinition of social inclusion patterns* in "European Journal of Research on Education," 2014, Vol. 2, No. 6, pp.109-115; Paladini Cristiana, *Circular migration and new forms of citizenship. The Albanian community's redefinition of social inclusion patterns*, "European Journal of Research on Education*",* 2014, Vol. 2, No. 6, https://www.semanticscholar.org/paper/Circular-migration-and-new-forms-of-citizenship.-of-Paladini/7d1db717a5ef331c85e97408dda57e7623fcd68b (10.09.2024)

[4]Alessandro Silj, *Albanese uguale criminale. Analisi critica di uno stereotipo*, in Limes 20 giugno 2001, https://www.limesonline.com/rivista/albanese--criminale--analisi-critica-di-uno-stereotipo-14578404/ (22.08.2024)

Argument	Clandestinenes	Work	Criminality	Intollerance	Bossi-Fini Law	Prostitution	Religion	Other arguments	TOTAL
No. articles	280	127	61	95	342	44	53	203	1.205
%	23.2	10.5	5.1	7.9	28.4	3.7	4.4	16.8	100,0

Table 3. Italy, Newspapers and Immigration: Articles by Subject (2002)[1]

Several studies contrasting media with actual crime rates and other problems have concluded that no link exists between media coverage and reality. However, it has been widely pointed out that media effects are very complex; it is not just that often they are different from the wishes of critics and researchers[2]. It is that they are different even from the portrayal of their enthusiasts. These findings have led to a growing interest in understanding how the media influences public perception and shapes societal norms. In response to the request for more specific information on how other issues were treated, particularly local events related to Albanians, it is crucial to delve deeper into the relationship between sensationalist coverage and the ignorance of the workings of bad reporting. This combination can often result in the exaggeration and distortion of the real circumstances of Albanians functioning in Italy. The consequences of such misrepresentation can be far-reaching, perpetuating stereotypes and hindering the integration process of Albanian communities.

To truly comprehend the impact of media coverage on public opinion, it is necessary to consider the underlying mechanisms that contribute to the formation of biased narratives. The sensationalism employed by certain media outlets not only captures attention but also distorts the realities faced by Albanians in Italy. By overemphasizing isolated incidents and amplifying negative experiences, media outlets inadvertently create a skewed perception of the Albanian community, leading to societal stigmatization and discrimination[3]. Furthermore, the lack of understanding and knowledge regarding the workings of bad reporting exacerbates the issue. Journalists who lack the necessary expertise or fail to conduct thorough research may unintentionally perpetuate false narratives about Albanians in Italy. This ignorance of the complexities and nuances of their experiences further fuels the misrepresentation and hinders accurate public understanding.

Addressing the misconceptions and misrepresentations surrounding the circumstances of Albanians in Italy necessitates a multifaceted approach. Firstly, media organizations must prioritize responsible reporting, ensuring that accurate information is conveyed to the public. Fact-checking and engaging with the Albanian community directly can help to avoid the dissemination of falsehoods and biases. Secondly, fostering dialogue and understanding between different communities can facilitate more accurate portrayals in the media. By promoting diversity and inclusivity, media coverage can become a tool for unity rather than division. In conclusion, while studies have shown no direct link between media coverage and reality, the complexity of media effects cannot be ignored. The combination of sensationalist coverage and ignorance of bad reporting practices can lead to the distortion and exaggeration of the circumstances faced by Albanians in Italy. To combat this issue, responsible reporting and fostering dialogue are vital steps towards promoting accurate narratives and facilitating the integration process of Albanian communities.

The institutional and policy framework of both sending and host countries is instrumental in shaping the nature, pace, and scale of migration. In fact, throughout history, states have played an immensely significant role in organizing and facilitating movement across borders, whilst also regulating labor rights. However, the willingness of these states to negotiate and accommodate largely determines whether migration occurs in an orderly or disorderly manner. Consequently, in the case of Albanian migration, the dichotomy

[1]Data processed on Caritas - *Migrantes XIII Rapporto sull'immigrazione*, Caritas di Roma, Rome 2003 https://www.simmweb.it/archivio-sito/fileadmin/documenti/Rapporti_immigrazione/caritas_dossier_statistico_immigrazione_03.pdf (11.09.2024)

[2]Phantom Cava Antonia, *Without a History: Immigrants and Media in Italy*, "Journalism and Mass Communication", Vol. 6, No. 10, 2016 https://pdfs.semanticscholar.org/4ce5/62efd19bebf979db6f20be60977a7e0694fa.pdf (11.09.2024)

[3]Mai Russell, *Italophilia meets Albanophobia: paradoxes of asymmetric assimilation and identity processes among Albanian immigrants in Italy*, "Ethnic and Racial Studies", 32(1), 2009, pp. 117-138 https://www.tandfonline.com/doi/abs/10.1080/01419870802245034 (11.09.2023)

between orderly and disorderly pertains to the various models that have shaped the movement patterns. Initially, the "roots-migration-enclave" model prevailed, wherein labor was quasi-imported to facilitate the subsequent social and spatial integration of migrants through family reunion. However, with time, alternative and more competitive models gained popularity, such as the "circular" or the "stepwise" migration model, which brought about distinct changes in the migration landscape[1]. These shifts resulted from the evolving attitudes of both sending and host countries, as well as the changing socioeconomic dynamics within Albania and its diaspora communities abroad. The exploration of these different models and their impact on Albanian migration provides valuable insights into the role of institutional frameworks, policy evolution, and sociopolitical factors in shaping migration patterns.

It was essentially these two models that EU member states applied when dealing with migration from former socialist countries. Beyond migration management, especially for the more recent "migration in turbulent times," institution-bilateral agreements are expected to promote social and economic rights to a more transitional kind of rights and responsibilities. Additionally, it is expected that the scope and scale of negotiations with countries of origin of temporary relocation with Albania will probably decrease considering the "sociodemographic decline of the EU"[2]. These changes warrant a comprehensive review and reevaluation of existing frameworks and mechanisms to ensure the successful management, integration, and coordination of migration policies and practices at both the regional and national levels. Furthermore, it is imperative to acknowledge the multifaceted nature of migration dynamics in the context of European Union member states.

As these dynamics continue to evolve, it becomes crucial to recognize the significance of socio-economic determinants that shape migration patterns and trends. By acknowledging these determinants, EU member states can better comprehend the complexities associated with migration and ensure that the appropriate policies and frameworks are in place to effectively manage and address them. Moreover, within the framework of migration management, it is crucial to consider the various factors that influence the social and economic rights of migrants. By promoting transitional rights and responsibilities, institution-bilateral agreements can contribute to the holistic integration of migrants into the host societies. This integration necessitates not only the provision of basic services but also opportunities for education, employment, and social participation, ensuring the long-term well-being and resilience of both migrants and host communities. Additionally, as the European Union experiences significant shifts in its geographical area of application, there is a pressing need to reevaluate the scope and scale of negotiations with countries of origin for temporary relocation[3].

The changing dynamics call for a comprehensive review of existing frameworks and mechanisms to ensure their relevance and effectiveness in the current socio-political landscape. This review should encompass a thorough examination of the legal and policy frameworks in place, as well as a critical analysis of national laws, regulations, and practices to ensure harmonization and coherence in migration management. Furthermore, the successful management, integration, and coordination of migration policies and practices necessitate a collaborative approach at both the regional and national levels. It requires close cooperation among EU member states, international organizations, civil society, and other stakeholders involved in migration governance. Through enhanced coordination mechanisms, knowledge-sharing, and capacity-building initiatives, the European Union can strengthen its collective response to the complex challenges posed by migration, ensuring a more equitable and inclusive society. In conclusion, the evolving nature of migration dynamics calls for a comprehensive and forward-looking approach to migration management within the European Union. By promoting transitional rights and responsibilities, reevaluating existing frameworks, and fostering collaboration among relevant stakeholders, the EU can effectively address the socio-economic complexities associated with migration and ensure the successful integration and well-being of both migrants

[1] Mai Russell, *Of myths and mirrors: Interpretations of Albanian migration to Italy*, "Studi Emigrazione", No. 39, 2002, p. 175, https://sussex.figshare.com/articles/journal_contribution/Of_myths_and_mirrors_interpretations_of_Albanian_migration/23321195 (01.08.2019)

[2] Niemann Zaun Natascha, *Introduction: EU external migration policy and EU migration governance*, "Journal of Ethnic and Migration Studies", Routledge 2023, pp.1-21 https://eprints.lse.ac.uk/119270/ (11.09.2024)

[3] Kahanec Ritzen, *A Sustainable Immigration Policy for the EU*, Springer, New York, 2017, p.157

and host communities. Only through such collective efforts can the European Union navigate the intricacies of migration in the present and lay the foundation for a more inclusive and prosperous future.

Conclusive remarks

This study examines evidence-based academic research published in various forums. More questions were raised about the impact of migration and trust between migrants and host societies, but not much work has been done on the social attitudes of Albanian migrants in Italy towards the host community. A poll conducted in Italy to address these issues in 2019 showed that social, economic, and cultural relations are closely linked. Albanian immigrants in Italy state that they have a good and warm relationship with the Italian community, but research shows evidence of existing ethnic, racial, and religious biases. This is difficult to measure through surveys, and the interaction between the policy, social, and communication development groups is not yet structured. It is crucial to explore the specific factors that shape their social attitudes towards the host community, considering variables such as length of stay, level of education, and socioeconomic status. By conducting in-depth interviews, focus groups, and ethnographic studies, we can gain valuable insights into the dynamics of their interactions and identify potential areas of improvement.

Moreover, policy responses need to be more targeted and tailored to address the existing biases and challenges faced by Albanian migrants in Italy. Measures should be implemented to promote inclusivity, eradicate discrimination, and foster intercultural dialogue. This requires a comprehensive approach that involves not only policymakers but also social and communication development groups. It is imperative to establish effective channels of communication between these stakeholders to ensure that policies are informed by empirical research and reflect the needs and aspirations of both migrants and the host community. Furthermore, educational initiatives can play a crucial role in promoting understanding and empathy between Albanian migrants and the Italian community.

By incorporating multiculturalism and diversity into the curriculum, schools can cultivate a more inclusive environment that celebrates different cultures, values, and identities. This will help combat the existing ethnic, racial, and religious biases and pave the way for a more harmonious coexistence. As Italy grapples with the challenges posed by the third immigration wave, it is crucial to address not only the fears and negative sentiments of the population but also the underlying factors contributing to these sentiments. A prevalent claim suggests that the interpersonal dynamics between “old” immigrant groups and Italians are more amicable compared to those with “new” groups that have recently settled in the country. This claim can be attributed to the long-standing intercultural policy of the nation, which has fostered better understanding and integration among established immigrant communities. Consequently, the Italian migration policy has proven to be periodic in nature, adapting to effectively navigate through tumultuous waves of immigration. The stricter approach has aimed to maintain order and uphold the rule of law. It is crucial to emphasize that these measures were not a reflection of prejudice against specific immigrant groups. Instead, they signified the political recognition of the importance of all citizens, including those from Albania, in shaping and implementing Italian border policies.

The example of the silent integration of Albanians, however, even if not supported by active policies in their favor, and marked by the visual and media impact that the landings via the Adriatic in 1991 had and the alarmist vision of the years to follow, demonstrates the possibility that a presumed invasion of workers in search of dignity can be transformed into a fruitful settlement (as demonstrated by the growing vitality of a business community, significant presence of students and professionals) and constitutes a heritage of good practices to be extended. It would take courage to adopt legislation that accelerates the obtaining of a residence permit and the reunification of family members at least for non-EU foreigners who graduated from university in Italy. We must also insist, with common sense, on the reform of the citizenship law and ensure that it remains on the parliamentary agenda, until the absurd situation is resolved by law in which Italianized children of parents who arrived in Italy as foreigners lose precious years in the bureaucratic process of coming of age to obtain the passport of the country they deserve to represent, even legally. Of course – and the Albanian case is there to demonstrate it – it is possible to achieve the integration of a foreign and even stigmatized community despite security and bureaucracy.

It is not right, however, to shoot ourselves in the foot by giving up harmonizing and merging diversity in a national community that is as rich as possible and equal in shared rights and duties. We must not forget the fact that foreign workers in Italy, because they are willing to make sacrifices and on average younger than the

population of the country where they work, pay more contributions to the treasury than the monetary benefits they receive. Where integration is in fact a reality, often positive and dynamic, the law should conform accordingly.

Bibliography

Books

1. Gemi, Eda; Triandafyllidou Anna, R*ethinking migration and return in Southeastern Europe: Albanian mobilities to and from Italy and Greece*, Routledge, London 2021
2. King, Russell; Mai, Nicola, *Out of Albania. From Crisis Migration to Social Inclusion in Italy*, Bergahn Books, Brooklyn NY, 2008
3. Ritzen, Jo; Kahanec, Martin, *A Sustainable Immigration Policy for the EU*, Springer, NY, 2017
4. Russell, King; Nicola, Mai, *The New Albanian Migrati*on, Sussex Academic Press, Brighton, 2005

Studies and Articles

1. Bonifazzi, Sabatino, *Albanian migration to Italy: what official data and survey results can reveal*, "Journal of Ethnic and Migration Studies", Vol. 29, No. 6,
2. Cava, Antonia, *Phantoms Without a History: Immigrants and Media in Italy*, "Journalism and Mass Communication", Vol. 6, No. 10, 2016
3. King, Russell, Mai, Nicola, *Italophilia meets Albanophobia: paradoxes of asymmetric assimilation and identity processes among Albanian immigrants in Italy*, "Ethnic and Racial Studies", Vol. 32, No. 1, 2009
4. King, Russell; Mai, Nicola, *Of myths and mirrors: Interpretations of Albanian migration to Italy*, "Studi Emigrazione" No. 39, 2002
5. King, Russell; Vullnetari, Julie, *Migration and Development in Albania*, "Sussex Centre for Migration Research", December, 2003
6. Niemann, Arne; Zaun, Natascha, *Introduction: EU external migration policy and EU migration governance*, "Journal of Ethnic and Migration Studies", Routledge, 2023
7. Paladini, Cristiana, *Circular migration and new forms of citizenship. The Albanian community's redefinition of social inclusion patterns*, "European Journal of Research on Education*",* Vol. 2, No. 6, 2014
8. Vathi, Zana, *The children of Albanian migrants in Europe: ethnic identity, transnational ties and pathways of integration*, University of Sussex, 2011

Documents

1. *Gazzetta Ufficiale del 28 Febbraio 1990, No. 49,* https://www.gazzettaufficiale.it/gazzetta/serie_generale/caricaDettaglio?dataPubblicazioneGazzetta=1990-02-28&numeroGazzetta=49
2. *Gazzetta Ufficiale No 199 del 26 agosto 2002 10 settembre 2002,* https://www.gazzettaufficiale.it/eli/gu/2002/08/26/199/sg/pdf
3. *Gazzetta Ufficiale n. 59 del 12 marzo 1998, Supplemento Ordinario No. 40,* https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1998-03-12&atto.codiceRedazionale=098G0066&elenco30giorni=false
4. Ministero del Lavoro e delle Politiche Sociali, Rapporto Comunità albanese in Italia. Rapporto Annuale dulla Presenza dei Migranti, 2023, https://www.lavoro.gov.it/sites/default/files/temi-e-priorita%2C%20immigrazione/studi-e-statistiche/RC_Albania_2023_def.pdf
5. Ministero del Lavoro e delle Politiche Sociali, *Rapporto Comunità albanese in Italia. Rapporto Annuale dulla Presenza dei Migranti*, 2022, https://www.lavoro.gov.it/sites/default/files/documenti-e-norme/studi-e-statistiche/RC-Albania-2022.pdf

Internet Sources

1. https://eprints.soton.ac.uk/
2. https://pdfs.semanticscholar.org/
3. https://sussex.figshare.com/

4. https://www.gazzettaufficiale.it/
5. https://www.lavoro.gov.it/
6. https://www.limesonline.com/
7. https://www.semanticscholar.org/
8. https://www.simmweb.it/
9. https://www.tandfonline.com/

Elena MÂRZAC
Moldova State University, Republic of Moldova

STRATEGIC COMMUNICATION AS A TOOL FOR COUNTERING HYBRID THREATS. A FOCUS ON NATIONAL RESILIENCE AND PUBLIC TRUST

Abstract:	*This paper examines strategic communication's important role in countering hybrid threats through early detection, real-time response, and collaboration among government, civil society, and technology sectors. Hybrid threats, such as foreign information interference, disinformation, cyberattacks, and political influence campaigns, present challenges to national security, particularly in the digital age. By fostering societal resilience and enhancing public trust in institutions, strategic communication frameworks are essential to safeguarding national interests. This paper explores how strategic communication frameworks can detect, respond to, and mitigate the impacts of hybrid threats, rapid and coordinated responses.* *Strategic communication can prevent the spread of disinformation, help build national resilience. By creating collaborative networks and using digital technologies, strategic communication protects national security and underscores their role in safeguarding national resilience. It aligns messaging across agencies, reinforcing government credibility during crises and fostering societal resilience through transparent, accurate information. By engaging with diverse audiences, StratCom adapts messages to influence positive public behaviors and build social cohesion. Additionally, it supports national interests by unifying government and societal efforts under clear objectives, while protecting information channels to secure communication. This proactive, coordinated approach strengthens democratic values and national security against hybrid threats.*
Keywords:	**Strategic communication; disinformation; hybrid threats; national interests; national resilience; societal resilience; social cohesion.**
Contact details of the authors:	E-mail: elena.marzac@gmail.com
Institutional affiliation of the authors:	**Moldova State University, Republic of Moldova**
Institutions address:	Alexei Mateeveci 60 street, Chișinau, MD-2009, tel: +37322244810, www.usm.md, rector@usm.md

Context of hybrid threats

Hybrid threats are complex, combining conventional and non-conventional tactics to destabilize social and political environments, often undermining public trust in government institutions and social cohesion[1]. Hybrid threats are not new, but their impact has become massive and dangerous in a globalized world with rapid communication development. The fundamental characteristic of hybrid aggression is that it is intended to exploit weaknesses and vulnerabilities within the political, economic and social systems, as well as in the critical infrastructures and information environments of the target state. Therefore, it is important for each state to be aware of its own vulnerabilities and to have the capacity to identify any changes in the public and

[1] Nicolas Jankowski, *Researching Fake News: A Selective Examination of Empirical Studies*, https://doi.org/10.1080/13183222.2018.1418964 (21.10.2024)

information security environment that could constitute elements of a foreign information interference campaign[1].

Hybrid threats are an umbrella term describing adversarial activities that blend military and non-military tactics, particularly in the digital and information domains. These activities exploit vulnerabilities within a state's cyber, political, and social infrastructures, often aiming to create confusion and erode public confidence in the government[2].

Hybrid tactics may include disinformation, cyber espionage, and political influence, complicating conventional defense mechanisms. In this regard, according to the Countering Hybrid Warfare in the Black Sea Region an effective institutional framework to counter hybrid threats needs to address four interconnected areas of action: (1) countering disinformation; (2) cybersecurity; (3) the resilience of critical infrastructure and supply chains; and (4) crisis and emergency management and defence[3].

The first two areas – countering disinformation and cybersecurity – have an impact on all aspects of social life. Securing the digital and information space requires inter-agency coordination and strengthening strategic communications capabilities. Additionally, sensitizing the public to the tools and effects of Russian disinformation is crucial for detecting and addressing the threat of hybrid warfare.

Achieving national resilience, including informational resilience to address hybrid threats, requires identifying key vulnerabilities and conducting a common risk assessment. This process demands a shared understanding of security threats and the synchronization of efforts among various state institutions. The war in Ukraine has clearly shown the importance of societal resilience, the existence of mechanisms for collaboration between the state and society, strategic communication, and efforts to prevent and combat propaganda and disinformation[4]. Effective defensive measures open immense opportunities for societies. Such threats are generally associated with foreign actors seeking to disrupt national stability through digital manipulation, cyberattacks, and disinformation campaigns[5]. Russia's influence in Eastern Europe, particularly in Moldova and Georgia, and disinformation efforts exemplify these tactics, where information manipulation has a profound impact on political stability[6].

These hybrid tactics are closely linked to information warfare, a phenomenon that Chifu and Simons argue that information warfare is made up of two parts that interact and influence one another—offensive and defensive components. For example, the offensive component is related to the goal of exploiting corrupting, denying, and destroying an adversary's information space. The goal is to advance the objectives and interests of the user. The defensive component concerns guarding, reinforcing, dominating, and enabling one's own information space, where the goal is to defend the objectives and interests of the user. Together, hybrid threats and information warfare represent a coordinated approach to achieving political influence, destabilizing adversaries in a volatile international and regional security environment.

In the current context of an increasingly interconnected world and vulnerable to information threats, Foreign Information Manipulation and Interference (FIMI) amplifies these risks, posing a growing threat to international security and stability. The concept of FIMI was developed by the European Union's (EU) European External Action Service (EEAS) in response to emerging threats, particularly those posed by Russian

---

[1] Viorica Ionela Trincu, *Contracararea amenințărilor hibride la nivelul Uniunii Europene, "*Gândirea Militară Românească", No. 2, 2019, p. 47

[2] *Understanding Hybrid Threats,* Helsinki, 2020, https://www.hybridcoe.fi/ (30.10.2024)

[3] *The Countering Hybrid Warfare in the Black Sea Region*, https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Countering_Hybrid_Warfare_Black_Sea_Region_ENG_fin.pdf p.12 (29.10.2024)

[4] *Reziliența în fața amenințărilor de tip hibrid. Un "sport de echipă" în care nimeni nu trebuie lăsat în urmă,* https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/ (29.10.2024)

[5] Iulian Chifu, Greg Simons, *Rethinking Warfare in the 21st Century. The Influence and Effects of the Politics, Information and Communication Mix,* https://www.cambridge.org/core/books/rethinking-warfare-in-the-21st-century/05181F92A0DFD584C1C609430F01B324 (29.10.2024)

[6] Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou, *The landscape of Hybrid Threats: A conceptual model*, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/ (29.10.2024)

disinformation campaigns[1]. FIMI refers to the intentional and coordinated efforts by state or non-state actors to manipulate information environments to achieve political, security, or other strategic objectives[2]. This concept covers not only disinformation, but also various forms of information manipulation and interference, which can undermine public trust in democratic institutions and affect political and social processes. The actors in such activity may be state or non-state actors, including their agents, either inside or outside their own territory[3].

For example, the EU's "Joint Framework on Countering Hybrid Threats" includes a very broad area of activities to counter hybrid threats, demonstrating the broadness of the field. The framework outlines several key areas: strategic communication to counter the systematic spread of disinformation; protection of critical infrastructures, such as energy supply chains and transportation, from unconventional attacks. This includes broad policy goals like diversifying the EU's energy sources, suppliers, and routes, ensuring transport and supply chain security, protecting space infrastructure from hybrid threats, and generally enhancing defense capabilities. Additionally, it emphasizes protecting public health and food security, including safeguards against chemical, biological, radiological, and nuclear (CBRN) threats. The framework also focuses on enhancing cybersecurity, with particular attention to industry, energy, financial, and transport systems. Furthermore, it addresses targeting the financing of hybrid threats and building resilience against radicalization and violent extremism[4].

In this article, we will refer to the role of strategic communication in countering hybrid threats and will demonstrate its important role. StratCom not only informs and raises awareness among the public, but also contributes to building social resilience by encouraging the adoption of positive and sustainable behaviors. The integration of strategic communication into information operations and intelligent data analysis are ways to develop coordinated and effective responses to information manipulations. In the specialized literature, we find several definitions of the concept. Christopher Paul defines strategic communication as a sum of "coordinated actions, messages, images, and other forms of signaling or engagement to inform, influence, or persuade selected audiences in support of national objectives"[5]. According to the author of the book "Corporate Communication," P.A. Argenti, who describes the concept of organizational communication (in our perspective, equivalent to strategic communication at the organizational level), defines the notion as "the solution through which employees can become more productive, and the created interaction provides management with greater credibility among employees"[6].

Strategic Communication is an indispensable informational element for national authorities. It emphasizes the state's efforts to understand and engage the target audience to create, strengthen, or maintain favorable conditions for advancing national interests, policies, and objectives. This involves coordinated communication—through programs, plans, themes, messages, and products—synchronized with the actions of all instruments of national power, both official and unofficial[7].

Various international organizations have also developed their own definitions of strategic communication. At the NATO level, strategic communication is understood as the coordinated and timely use of communication activities and capabilities-public diplomacy, public relations, information operations, and

[1] *Tackling Online Disinformation: An European approach*, https://ec.europa.eu/information_society/newsroom/image/document/2018-28/presentationcomm_paolo_cesarini_202D869F-9A13-6D79-FC46C00EAAE3E9AC_53429.pdf (28.10.2024)

[2] *Foreign Information Manipulation and Interference (FIMI)*, https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html (18.11.2024)

[3] Bernard Siman, *Countering FIMI: A Critical Imperative for Mission Safety*, https://www.egmontinstitute.be/countering-fimi-a-critical-imperative-for-mission-safety/ (22.10.2024)

[4] European Union, *Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (22.10.2024)

[5] Christopher Paul, *Getting Better at Strategic Communication*, Rand Corporation, Pittsburgh, 2011

[6] Paul Argenti, *Corporate Communication*, Irwin McGraw-Hill, Boston, 1998, p. 17

[7] Kenneth E. Kim, *Framing as a Strategic Persuasive Message Tactic*, "The Routledge Handbook of Strategic Communication", p. 285, https://www.routledge.com/The-Routledge-Handbook-of-Strategic-Communication/Holtzhausen-Zerfass/p/book/9780367367732?srsltid=AfmBOoqL8zgYUO5NOK1a7-8-uH_JtsTvFBGTjeO-v2F-G1M3eaqSE4AP (22.10.2024)

psychological operations, as necessary, to support NATO policies, operations, and activities and to achieve Alliance objectives[1].

Defined broadly, strategic communication is a framework used to align governmental and societal messaging in a manner that counters adversarial narratives and enhances resilience. It involves targeted messaging, stakeholder engagement, and the use of digital platforms to bolster national security against hybrid threats. Through strategic communication, governments can build a narrative that counters misinformation effectively[2]. Strategic communication has emerged as an essential tool for counteracting hybrid threats, involving the use of coordinated messaging to protect national interests and maintain social cohesion. StratCom supports both proactive and reactive approaches, equipping governments and institutions with the capacity to inform, educate, and engage the public effectively[3].

Strategic communication: diverse approaches

The process is designed to counter the disruptive effects of disinformation and malicious information, targeting not only the external public, to promote national interests, but also the internal public, to increase its resilience to information attacks. Process integrated into a large-scale initiative, encompasses multidisciplinary and social marketing, non-formal education, public participation, aimed at innovative and sustainable change of practices, behaviors and lifestyles, guides communication processes and media interventions among social groups and is a prerequisite and a tool for change at the same time.

StratCom is a process that interconnects democratic values, public institutions, supra-state institutions, the media, and various national and international categories of public. This requires an understanding of relevant actors, their strategic objectives, the measures they employ and which of our own vulnerabilities might be exploited. All of these are wrapped up in the narratives adopted by any hostile actor, designed to target different audiences[4]. StratCom can be an option for changing people's way of thinking, which in addition to voluntary involvement and unconditional assumption of responsibility, first, also includes continuous adaptability and flexibility to keep up with the expansion and diversification of the hybrid phenomenon. Ideally, it should be established at the highest leadership level within a state, organization, or institution and should be communicated and implemented effectively down to the lowest tactical level. Its role is to educate and inform the public, but, more than that, the most effective kind of strategic communication changes behaviors[5]. To effectively counter hybrid threats, strategic communication plays a critical role by serving multiple functions that work together to enhance national resilience. These functions include:

1. Early Detection and Monitoring

One of the most effective uses of strategic communication is early detection. By employing monitoring tools across social media and other digital platforms, governments can detect hybrid threats before they escalate. Real-time monitoring, coupled with data analytics, provides a foundation for rapid response strategies[6], integrating these approaches allows governmental and non-governmental agencies to counteract disinformation campaigns and manage crises proactively. The European Union has implemented several measures for the early detection and monitoring of disinformation. For example, the EU Code of Practice on Disinformation (established in 2018 and strengthened in 2022), involves commitments from online platforms, trade associations, and the advertising sector to curb disinformation. It includes measures to improve transparency, empower users, and enhance cooperation with fact-checkers.[7]. Other successful could be

[1]NATO, *ACO Strategic communications* AD 95-2/21 May 2012, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf (22.10.2024)

[2]Andrew, Chadwick, *The Hybrid Media System. Politics and Power*, Oxford University Press, Oxford 2017, p. 43

[4]*Strategic communications hybrid threats toolkit. Comunications to understand and counter grey zone threats*, https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf (22.10.2024)

[5]Elena Mârzac, Sanda Sandu, *Comunicarea strategică – instrument de fortificare a rezilienței informaționale*, "Reziliența în atenția securității. Concepte, procese, necesități", USM, Chișinău, 2022, p. 66

[6]Dakota Cary, Daniel Cebul, *Destructive Cyber Operations and Machine Learning***,** https://cset.georgetown.edu/publication/destructive-cyber-operations-and-machine-learning/ (22.10.2024)

[7] *A strengthened EU Code of Practice on Disinformation*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en (22.10.2024)

considered the Action Plan Against Disinformation, launched in 2018, this plan focuses on improving detection, analysis, and exposure of disinformation. It also emphasizes stronger cooperation between Member States and EU institutions, as well as mobilizing the private sector to tackle disinformation[1].

2. Coordination and Rapid Response

Strategic communication, as a process, can contribute to a more effective orchestration of government activities, integrating various activities within the instruments of power, in order to strategically influence and form national resilience. Integration of efforts between all instruments of power: diplomatic, informational, military and economic, based on the national security strategy and risk and threat assessment.

Strategic communication aims to influence, and strategic influence depends entirely on effective coordination between the government and, beyond it, to achieve national strategic objectives. Given the central influence on the national strategy, a strategic communication framework must be present in strategic planning and in the preparation and implementation of policies[2].

Strategic communication enables a coordinated response to hybrid threats by creating a unified message across multiple agencies and sectors. It requires a high level of coordination across different strategic, operational, and tactical levels. This ensures that all communication efforts are aligned and reinforce each other[3]. For instance, the EU's "East StratCom Task Force" was established to monitor and counteract Russian disinformation campaigns, ensuring that coordinated, accurate messaging reaches European citizens.

3. Building Public Trust and Social Cohesion

Strategic communication serves to build resilience by fostering public trust through transparency and accountability. When governments deliver credible and timely information, they are better positioned to gain public support. Studies demonstrate that consistent, truthful communication helps mitigate the influence of adversarial misinformation[4]. Moreover, societal resilience is strengthened when citizens are informed and can differentiate between authentic information, disinformation, and manipulation. Effective, citizen-centred public communication can help build trust in democratic institutions by ensuring and demonstrating that the government is reliable, responsive, open and fair. It is an essential asset to prevent and counteract mis- and disinformation, along with other governance responses[5]. Strategic communication is a two-way process, which conveys the reactions and points of view of the different audiences involved in the communication process. Public feedback should be used for regular policy and strategy adjustments. More ambitiously, strategic communication is not limited only to media messages; it must contribute to the development of a communication campaign oriented towards behavioral or social changes of the public. That is why effective strategic communication presumes identification, understanding and engagement with target audiences. This process involves deep knowledge of their needs, values, fears, beliefs, and behaviors that would allow bettering to reach the audience, to adjust the messages and to identify better channels of communication.

It is necessary to identify and coordinate all governmental instruments (political leaders, decision-makers, strategic actors, communicators, implementing actors, official diplomacy, public affairs, media operations, public-private partnership, military diplomacy, internal communication, interdepartmental public relations), as well as societal instruments (media, NGOs, private communication entities, academia, cultural institutions, business, public figures, influential authors, scientists, the diaspora, etc.).

Strategic communication is an indispensable tool in the process of good governance and development of the Republic of Moldova, both for streamlining the governing act and for ensuring common communication and understanding between all stakeholders. Good governance assumes that states institutions must be transparent in decision-making and accountable for their actions, correctly and impartially implement laws to

---

[1] *Action plan against disinformation. Report on progress*, https://ec.europa.eu/commission/presscorner/api/files/attachment/857709/factsheet_disinfo%20elex_140619%20final.pdf (22.10.2024)

[2] Elena Mârzac, Sanda Sandu, *Op. cit.*, p. 66

[3] European Parliament, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[4] Lance Bennett, Steven Livingston, *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication", Vol. 33, No. 2, 2018, p. 129

[5] *Good practice principles for public communication responses to mis- and disinformation*, https://www.oecd-ilibrary.org/governance/good-practice-principles-for-public-communication-responses-to-mis-and-disinformation_6d141b44-en (20.11.2024)

maintain order and protect citizens' rights, reform the judiciary to ensure the independence of the judiciary and fight corruption, etc. An indicator of good governance is the active involvement of citizens in political and social processes, both through public consultations, citizens' initiatives and by supporting a strong civil society.

Without communication structures and processes that allow the exchange of information between the state and citizens, it is difficult to imagine that states can be responsive to the needs, expectations, and needs of the public. Trust has played an important role in effectively managing the COVID-19 pandemic, as countries with higher levels of social and government trust have typically seen slower virus spread and a lower mortality rate[1]. As trust rises, so does confidence in government information generally, enabling a unified response and increased citizen cooperation.

Since the start of the pandemic, Singapore has focused on clear and consistent information sharing. The government had an effective communication plan: The members of the COVID task force held daily press conferences, during which they explained the evolving COVID-19 situation and resulting government decisions[2]. Data trusts and data-sharing infrastructure, such as Estonia's X-tee platform, build public trust by facilitating the secure and authenticated exchange of data. Estonian public sector organizations are required to use the heavily regulated X-tee tool to access or share data. This platform improves cohesion across government agencies and bolsters citizen confidence[3]

4. Promoting national interests and supporting the implementation of national policies and objectives.

Given the current risks and threats, as well as national interests, strategic communication is an essential piece of information for national authorities and is one of the tools that the state uses to achieve its objectives. The promotion of national interests depends on the continued efforts of state and non-state actors to coordinate messages and actions and how all stakeholders will perceive them in the national security and defence sector.

In the absence of effective strategic communication, national interests are compromised, political changes lead to deviations, and the population becomes vulnerable to disinformation and manipulation. Additionally, the lack of a clear international vision generates domestic skepticism, facilitating propaganda and confusion among foreign partners. The lack of StratCom can generate incoherence and chaos in actions and messages, with serious consequences, as strategic communication supports the implementation of national strategies and counteracts conflicts, including hybrid wars, being vital for achieving the political, economic, social, security and defense objectives of the state. Effective communication reflects and supports good governance. Effective coordination and the delivery of the right messages, in line with the strategic objectives of the state and its institutions, will help align the efforts of the various national entities and strengthen cohesion in different sectors, with a view to countering disinformation.

The integration of a common mentality of strategic communication at all levels of state institutions and implementation of the national strategy will determine a high strategic culture, which will facilitate the necessary changes in the current practice. Thus, strategic communication can become a powerful tool of power, used to shape attitudes and behaviors, to listen to and understand the public, and to coordinate messages between the government and its partners, ensuring an effective integration of information with other instruments of national power[4]. In this regard, StratCom can accelerate, influence and improve citizens' perceptions of certain vital areas for the country's development, understanding the actions of decision-makers, raising awareness and supporting certain reforms.

For the Republic of Moldova, strategic communication and combating information manipulation through FIMI are critical due to its position between the European Union and the Russian Federation. Moldova is particularly vulnerable to disinformation campaigns aimed at destabilizing society and undermining trust in

[1] Thomas Bollyky, *Fighting a pandemic requires trust: Governments have to earn it*, "Foreign Affairs", October 23, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-23/coronavirus-fighting-requires-trust, (20.11.2024)

[2] Jeremy Lim, *How Singapore is taking on COVID-19*, "Asian Scientist Magazine", April 3, 2020, https://www.asianscientist.com/2020/04/features/singapore-covid-19-response/ (20.11.2024)

[3] Bruce Chew, Michael Flynn, Georgina Black, Rajiv Gupta, *Sustaining public trust in government*, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2021/public-trust-in-government.html, (20.11.2024)

[4]Elena Marzac, Viorica Zaharia, *Comunicarea strategică și combaterea dezinformării. Ghid de combatere a dezinformării prin comunicare strategică*, Bons Office, Chișinău, 2024, p. 12

democratic institutions[1]. FIMI seeks to provoke political and ethnic tensions, leading to polarization and hindering the implementation of democratic, economic, and security reforms. Additionally, in the context of national security, disinformation fosters confusion and uncertainty, eroding public confidence in the state's capacity to address pressing challenges.

According to the National Security Strategy, the Republic of Moldova faces several threats to national security, including the hybrid operations carried out by the Russian Federation against the Republic of Moldova in the political, economic, energy, social, informational, cyber fields, etc., with the aim of undermining the constitutional order, derailing the country's European course and/or disintegrating the state[2]. In addition, Moldova, in the desire to integrate with the European Union and to maintain stable relations with its neighbors, is subject to information manipulation, which can influence public opinion and hinder pro-European policies. Thus, strengthening strategic communication is an important action in protecting democratic values, maintaining social cohesion and increasing resilience to external threats.

5. Strategic communication is vital in countering disinformation campaigns as it is a process designed, among other things, to counter the disruptive effects of disinformation. It targets not only external audiences with the aim of promoting national interests but also internal audiences to enhance resilience against national attacks.

The process of strategic communication can be the opportunity needed to stop the evolution of certain currents, to increase the public's resilience to disinformation campaigns and to promote certain basic narratives/messages regarding the national interests of the state among the population. For example, the European Commission is strengthening its strategic communication to combat disinformation, manipulation of information from outside and foreign interference targeting EU policies. This requires a whole-of-society approach, as many sectors play an important role in preventing and combating disinformation. It is also important to ensure that citizens have access to quality and trustworthy news and information[3]. In this regard, the Commission, among others, is directing its efforts in the fight against disinformation by developing policies aimed at strengthening European democracies, making it harder for disinformation actors to misuse online platforms, protecting journalists and media pluralism, countering foreign interference and cyberattacks through awareness-raising projects, advanced technological solutions, and better coordination, and strengthening society's resilience against disinformation through media literacy and awareness-raising initiatives[4].

For instance, the EU's StratCom East Task Force has been effective in countering Russian disinformation campaigns targeting Eastern European countries, including Moldova. This initiative involved monitoring and exposing disinformation narratives, as well as providing alternative, fact-based information to local populations[5].

Another example is the NATO Strategic Communications Centre of Excellence, which has supported member states in developing their own StratCom capabilities. Their efforts in Ukraine during the 2014 crisis and Russian war in Ukraine started in February 2022 are a prime example of how coordinated communication can counteract propaganda and support democratic resilience in the face of external threats. Similarly, in the Republic of Moldova, efforts have been made to institutionalize strategic communication and respond to the challenges associated with fake news, propaganda, and disinformation campaigns. To this end, in the Republic

---

[1] *Blurring the Truth: Disinformation in Southeast Europe*, https://www.kas.de/documents/281902/281951/E-book+Blurring+the+Truth.pdf/fd6abbb3-f49e-115b-090e-7c9f3a20dfc6?version=1.2&t=1680504776349%20Blurring%20the%20Truth:%20Disinformation%20in%20Southeast%20Europe (30.09.2024)

[2] Parlamentul Republicii Moldova, *Strategia Națională de Securitate a Republicii Moldova*, https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf (30.09.2024)

[3] *Comunicare strategică și combaterea dezinformării*, https://commission.europa.eu/topics/strategic-communication-and-tackling-disinformation_ro (26.10.2024)

[4] Parlamentul Republicii Moldova, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[5] Kristina Berzina, Kovalcikova Nada, David Salvo, Soula Etienne, *European policy blueprint for countering authoritarian interference in democracies*, https://www.jstor.org/stable/pdf/resrep21251.8.pdf?refreqid=excelsior%3A2a2bf2246650062af2b9851a5db9023 (30.09.2024)

of Moldova, the Center for Strategic Communication and Combating Disinformation was created in July 2023. The Center's mission is to increase efforts in combating specific actions that pose a threat to national interests.

According to the Concept of Strategic Communication and Countering Disinformation for 2024-2028[1], the need for an institutionalized and integrated approach to strategic communication and countering disinformation in the context of external and internal threats faced by the Republic of Moldova, especially from the Russian Federation, was argued. The vision consists of "supporting, consolidating and contributing to the achievement of national interests, which are the foundations of the idea of the Republic of Moldova as a state of the century. The concept has the following general objectives: to develop the institutional capacities of the state and society to communicate effectively and combat disinformation. The main thematic areas addressed are: European integration, social cohesion, economic resilience, strengthening the defense sector and strengthening national security in the regional context.

This integrated and action-oriented approach aims to strengthen the democracy, security and socio-economic development of the Republic of Moldova in the coming years. An important argument for supporting the importance of strategic communication as a tool to counter hybrid threats that negatively impact national security, is the fact that the national security strategy of the Republic of Moldova[2].

Beyond informing, strategic communications aim to influence and promote specific behaviors. This can be crucial in situations where public cooperation is needed to counter hybrid threats[3]. The strategic mindset in communication also implies an integrated vision, which combines persuasive strategies with participatory practices. It is not limited to one-way communication, but promotes dialogue and engagement, recognizing the importance of building new realities through the active involvement of the public. In a world where many external factors compete for influence in a complex information environment, strategic communication must be flexible and adaptable, able to respond to challenges proactively and creatively.

Strategic communication communicates "narratives". Narratives, according to Lawrence Freedman, are conceived or cultivated with the intention of structuring audiences' responses to certain events, therefore, narratives refer to influence. Narratives are stories that make sense to the audience because they relate to shared values and experiences, however, in the long run they can be used to shape an audience's perceptions and interests. Realized at the strategic level, narratives are a means for political actors to build a common sense of the past, present and future of international politics to shape domestic behavior and international actors. Strategic narratives can be used to communicate the "soft power" that a country wants to design. Indeed, according to Roselle, strategic narrative is soft power in the 21st century.

Key approaches to strategic communication in hybrid threat scenarios

To deter hybrid threats, it is necessary to take several proactive and reactive measures that are interdependent. To achieve them, specific capabilities are needed to cover all the essential functions necessary to counter hybridity in a timely manner, as early as possible, such as: monitoring, detecting, identifying, disclosing and rejecting any hybrid actions and activities. These capabilities give weight to the approach and increase the determination to react and fight back when the relaunched competition and the influence sought by hybridity exceed any limit of bear ability in the target state. Without these capabilities to ensure early detection and timely intervention to counter hybrid threats, regardless of the volume of communication involved, there would most likely not be enough credibility framework.

On the other hand, beyond the presentation and promotion of these specific capabilities and their overall effectiveness, there is another facet of credibility, namely political determination, the willingness to

[1]Parlamentul Republicii Moldova, *Hotărâre privind aprobarea Concepţiei de comunicare strategică și contracarare a dezinformării, a acţiunilor de manipulare a informaţiei și a ingerinţelor străine pentru anii 2024–2028*, https://www.parlament.md/LegislationDocument.aspx?Id=25cfe6b6-795d-47eb-82a3-065d51d26fdf (30.09.2024)

[2] Parlamentul Republicii Moldova, *Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și modificarea unor acte normative*,
https://presedinte.md/app/webroot/uploaded/Proiect%20Lege%20Centrul%20CSC%20Dezinformare%2005.07.23.pdf (26.10.2024)

[3]*Hybrid Threats: A Strategic Communications Perspective - StratCom COE*, https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79 (26.10.2024)

.

point the finger at the hybrid aggressor and publicly disclose hybrid actions. StratCom is involved in this process by delivering appropriate messages that serve its own purposes. The process must be organized in a synchronized, coherent manner, so that the target audience can anticipate, be prepared, involved and proactively against hybrid actions. Proactive measures, including awareness campaigns and digital literacy programs, play an essential role in preparing the public to identify and resist disinformation. These efforts are akin to "inoculating" the population against false narratives by preemptively educating citizens on recognizing misinformation tactics. Public awareness campaigns on social media can demystify misinformation and guide citizens toward credible sources, strengthening resilience against hybrid threats[1].

In scenarios where hybrid threats are already present, governments must employ targeted reactive measures. Strategic communication can include rebuttal campaigns, rapid fact checking, and coordinated messaging to counteract narratives already circulating within the information ecosystem. By establishing a rapid response system, governments can swiftly correct misinformation, reducing its impact on the public[2].

Digital platforms play a crucial role in the dissemination of strategic communication. Through data-driven insights and targeted outreach, governments can respond to threats more effectively. Artificial intelligence (AI) enhances the detection of threats and assists the strategic communication specialists to adjust the strategies, tailor the messages and to understand the emotions and in result to shape the perceptions. AI and machine learning algorithms can process vast amounts of data to identify patterns and predict future trends. This enhances the strategic planning and execution of communication campaigns[3]. IAI-driven tools can automate the detection and countering of disinformation, making information operations more efficient and scalable[4].

Artificial intelligence plays a double role here, as it can be used by both the promoters of hybrid threats to develop attacks that are more sophisticated and by defenders to counter them. AI can be used to create and spread false content (text, images, audios, videos) without human intervention, which could accelerate and reduce the costs of disinformation campaigns. It is also a key technology used in detecting and preventing disinformation and other components of hybrid *threats*. The European Union's experience with strategic communication highlights the necessity of a coordinated response to hybrid threats. The EU's East StratCom Task Force, established in 2015, has been instrumental in monitoring and countering FIMI specifically targeting Russian influence operations in Eastern Europe[5]. This initiative underscores the effectiveness of regional collaboration in combatting hybrid threats through strategic communication.

While StratCom is crucial for ensuring clarity in activities, engaging diverse target audiences and stakeholders, managing crises, and enhancing overall efficiency, it also presents challenges and limitations. One major challenge is information overload, where an audience inundated with excessive information may experience fatigue and disengagement. A relevant example is the overwhelming flow of information about the war in Ukraine in Central and Eastern Europe[6]. Therefore, it's crucial to balance the volume of communication and ensure that messages are concise and impactful for the specific target audiences. Prioritizing information is also essential to ensure that the most critical messages are delivered effectively.

Another significant challenge is coordinating communication efforts across multiple stakeholders, including departments, teams, and external partners. This complexity demands clear protocols and effective management to ensure alignment. Maintaining consistency in strategies and messages across large organizations further complicates the process. For instance, in organizations like NATO or EU, different members may convey messages that deviate from agreed-upon frameworks. Similarly, challenges arise in states where StratCom is not adequately institutionalized, leading to fragmented or conflicting communication.

---

[1] Andrew Chadwick, *Op. cit*., p. 45

[2] Richey Mayson, *Disinformation and Strategic Communication in Hybrid Warfare*, "Journal of Strategic Studies", Vol. 12, No. 1, 2021, p. 78

[3] *AI in Support of StratCom Capabilities*, https://stratcomcoe.org/pdfjs/?file=/publications/download/Revised-AI-in-Support-of-StratCom-Capabilities-DIGITAL---Copy.pdf?zoom=page-fit (22.11.2014)

[4] US Department of Defence, *Strategy for operations in the information environment, 2023*, https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF (22.11.2024)

[5] European Parliament, *Strategic communications as a key factor in countering hybrid threats*, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323 (30.09.2024)

[6] Claudia Ciobanu, Jules Eisenchteter, Nicholas Watson, Edit Inotai, *War fatigue in central Europe is spreading*, https://balkaninsight.com/2024/07/01/war-fatigue-in-central-europe-is-spreading/ (22.11.2024)

Coordinating a coherent strategic message is further complicated by new media outlets such as blogs, chat rooms and text messaging, which are becoming preferred sources for information-regardless of validity-in some demographic groups and make "managing" information release impossible[1]. StratCom also requires significant resources. Developing and implementing a strategic communication plan can be time-consuming and costly, requiring investment in skilled personnel and technology. Continuous training is necessary to keep the communication team updated on best practices and emerging trends.

In our opinion one of the most important barriers is the Resistance to change. Employees and other stakeholders might resist new communication strategies, preferring familiar practices. This is particularly challenging in multinational organizations (e.g. NATO, EU, OSCE), where cultural differences can hinder the implementation of a unified communication strategy. Finally, measuring effectiveness poses its own challenges. Identifying the right metrics to assess the effectiveness of strategic communication can be complex. States and organizations need to establish clear goals and balance qualitative and quantitative data to make informed decisions.

Conclusions

Strategic communication is one of the indispensable instruments in countering hybrid threats. By enabling the timely and accurate transmission of information, StratCom frameworks build public trust, enhance resilience, and safeguard national security. The coordinated use of stakeholder engagement, coordination communication activities help governments to counteract FIMI, disinformation, mitigate cyber threats, and strengthen societal cohesion, thus, to obtain the support for governmental decisions and reforms.

Strategic communication is key for effectively countering hybrid threats and promoting a safer and more informed society, helping to protect national security and state integrity. StratCom in the fight against FIMI contributes to protecting democratic values and increasing social resilience. By integrating data analytics and information operations, StratCom develops coordinated and effective responses to disinformation campaigns, facilitating collaboration between governments, NGOs and local communities. These efforts make it possible not only to combat information threats, but also to change behaviors and promote social cohesion, which are essential for long-term democratic stability.

Strategic communication not only provides the necessary framework for the rapid and accurate transmission of messages, but also strengthens society's resilience by educating and informing the public.

In addition, by disseminating the right messages and using digital technologies, strategic communication can counter propaganda and disinformation and support efforts to ensure security. Moreover, while StratCom provides substantial benefits, overcoming challenges such as information fatigue, uncoordinated messaging, and limitations in human and technical resources requires meticulous planning, efficient management, and a commitment to continuous improvement.

Bibliography

Books

1. Argenti, Paul, *Corporate Communication*, Irwin McGraw-Hill, Boston, 1998
2. Chadwick, Andrew, *The Hybrid Media System. Politics and Power,* Oxford University Press, Oxford 2017
3. Chifu, Iulian; Simons, Greg, *Rethinking Warfare in the 21st Century*, Cambridge University Press, Cambridge, 2013
4. Marzac, Elena; Zaharia, Viorica, *Comunicarea strategică și combaterea dezinformării. Ghid de combatere a dezinformării prin comunicare strategică*, Bons Office, Chișinău, 2024
5. Paul, Christopher, *Getting Better at Strategic Communication*, Rand Corporation, Pittsburgh, 2011

[1] Michael, A. Brown, *Challenges of Strategic Communication*, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1171&context=ils (23.11.2024)

Studies and Articles

1. Bachmann, Sascha-Dominik; Gunneriusson, Hakan. *Hybrid Warfare: The Law and Policy of Leveraging Non-Military Elements*, "Journal of Strategic Security", Vol. 14, No. 2, 2017
2. Bachmann, Sascha-Dominik; Putter, Dries; Duczynsk, Guy, *Hybrid warfare and disinformation: A Ukraine war perspective*, https://doi.org/10.1111/1758-5899.13257
3. Bennett, Lance; Livingston, Steven, *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication", Vol. 33, No. 2, 2018
4. Bollyky, Thomas, *Fighting a pandemic requires trust: Governments have to earn it* , "Foreign Affairs", October 23, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-23/coronavirus-fighting-requires-trust
5. Kim, Kenneth E., *Framing as a Strategic Persuasive Message Tactic*, "The Routledge Handbook of Strategic Communication", 2015, https://www.routledge.com/The-Routledge-Handbook-of-Strategic-Communication/Holtzhausen-Zerfass/p/book/9780367367732?srsltid=AfmBOoqL8zgYUO5NOK1a7-8-uH_JtsTvFBGTjeO-v2F-G1M3eaqSE4AP
6. Lim, Jeremy, *How Singapore is taking on COVID-19*, "Asian Scientist Magazine", April 3, 2020, https://www.asianscientist.com/2020/04/features/singapore-covid-19-response/
7. Mârzac, Elena; Sandu, Sanda, *Comunicarea strategică – instrument de fortificare a rezilienței informaționale,* "Reziliența în atenția securității. Concepte, procese, necesități", USM, Chișinău, 2022
8. *Reziliența în fața amenințărilor de tip hibrid. Un "sport de echipă" în care nimeni nu trebuie lăsat în urmă*, https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/
9. Trincu, Viorica, Ionela, *Contracararea amenințărilor hibride la nivelul Uniunii Europene*, "Gândirea Militară Românească", No. 2, 2019

Documents

1. *Action plan against disinformation. Report on progress*, https://ec.europa.eu/commission/presscorner/api/files/attachment/857709/factsheet_disinfo%20elex_140619%20final.pdf
2. Bachmann, Sascha-Dominik, *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats– mapping the new frontier of global risk and security management*, https://www.researchgate.net/publication/228214544_Hybrid_Threats_Cyber_Warfare_and_NATO%27s_Comprehensive_Approach_for_Countering_21st_Century_Threats_-_Mapping_the_New_Frontier_of_Global_Risk_and_Security_Management
3. *Blurring the Truth: Disinformation in Southeast Europe*, https://www.kas.de/documents/281902/281951/E-book+Blurring+the+Truth.pdf/fd6abbb3-f49e-115b-090e-7c9f3a20dfc6?version=1.2&t=1680504776349%20Blurring%20the%20Truth:%20Disinformation%20in%20Southeast%20Europe
4. Cary, Dakota; Cebul, Daniel, *Destructive Cyber Operations and Machine Learning***,** https://cset.georgetown.edu/publication/destructive-cyber-operations-and-machine-learning/
5. Chew, Bruce; Flynn, Michael; Black, Georgina; Gupta, Rajiv, *Sustaining public trust in government*, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2021/public-trust-in-government.html
6. Ciobanu, Claudia; Eisenchteter, Jules; Watson, Nicholas; Inotai, Edit, *War fatigue in central Europe is spreading*, https://balkaninsight.com/2024/07/01/war-fatigue-in-central-europe-is-spreading/
7. *Comunicare strategică și combaterea dezinformării*, https://commission.europa.eu/topics/strategic-communication-and-tackling-disinformation_ro
8. Doncheva, Tihomira; Svetoka, Sanda, *Russia's Footprint in the Western Balkan Information Environment: Susceptibility to Russian Influence*, https://stratcomcoe.org/publications/russias-footprint-in-the-western-balkan-information-environment-susceptibility-to-russian-influence/216
9. *East StratCom Task Force in the Strategic Communication, Task Forces and Information Analysis*. https://www.eeas.europa.eu/eeas/contract-agent-fg-iii-post-strategic-communications-assistant-east-stratcom-task-force-strategic_und_en

10. European Parliament, *Strategic communications as a key factor in countering hybrid threats*, 2021, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656323
11. European Union, *Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council*, https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:52016JC0018R(01)
12. *Foreign Information Manipulation and Interference (FIMI)*, https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html
13. Giannopoulos, Georgios; Smith, Hanna, Theocharidou Marianthi, *The landscape of Hybrid Threats: A conceptual model*, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/
14. *Good practice principles for public communication responses to mis- and disinformation*, https://www.oecd-ilibrary.org/governance/good-practice-principles-for-public-communication-responses-to-mis-and-disinformation_6d141b44-en
15. *Hybrid Threats: A Strategic Communications Perspective - StratCom COE*. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79,
16. Jankowski, Nicolas W., *Researching Fake News: A Selective Examination of Empirical Studies*, https://doi.org/10.1080/13183222.2018.1418964
17. Lucas, Edward; Pomerantsev, Peter, *Winning the Information War*, https://cepa.org/comprehensive-reports/winning-the-information-war/
18. NATO, *ACO Strategic communications AD 95-2/21 May 2012*, https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf
19. Parlamentul Republicii Moldova, *Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și modificarea unor acte normative*, https://presedinte.md/app/webroot/uploaded/Proiect%20Lege%20Centrul%20CSC%20Dezinformare%2005.07.23.pdf
20. Parlamentul Republicii Moldova, *Strategia Națională de Securitate a Republicii Moldova*, https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf
21. Siman, Bernard, *Countering FIMI: A Critical Imperative for Mission Safety*, https://www.egmontinstitute.be/countering-fimi-a-critical-imperative-for-mission-safety/
22. *Strategic communications hybrid threats toolkit. Comunications to understand and counter grey zone threats*, https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf
23. *Tackling Online Disinformation: An European Approach*, https://ec.europa.eu/information_society/newsroom/image/document/2018-28/presentationcomm_paolo_cesarini_202D869F-9A13-6D79-FC46C00EAAE3E9AC_53429.pdf,
24. *The Countering Hybrid Warfare in the Black Sea Region*, https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Countering_Hybrid_Warfare_Black_Sea_Region_ENG_fin.pdf
25. *The Influence and Effects of the Politics, Information and Communication Mix*, https://www.cambridge.org/core/books/rethinking-warfare-in-the-21st-century/05181F92A0DFD584C1C609430F01B324
26. *Understanding Hybrid Threats*, Helsinki, 2020. https://www.hybridcoe.fi/
27. US Department of Defence, *Strategy for operations in the information environment, 2023*, https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF
28. Weissmann, Mikael, *Conceptualizing and countering hybrid threats and hybrid warfare*, https://www.academia.edu/83737397/Conceptualizing_and_countering_hybrid_threats_and_hybrid_warfare?nav_from=39e5c9a6-48a6-443e-8135-8ce4d77af977

Websites

1. https://cepa.org/
2. https://commission.europa.eu/
3. https://csd.eu/

4. https://cset.georgetown.edu/
5. https://e-arc.ro/
6. https://ec.europa.eu/
7. https://ec.europa.eu/
8. https://eur-lex.europa.eu/
9. https://media.defense.gov
10. https://presedinte.md/
11. https://stratcomcoe.org/
12. https://stratcomcoe.org/
13. https://www.academia.edu/
14. https://www.act.nato.int/
15. https://www.asianscientist.com/
16. https://www.eeas.europa.eu/
17. https://www.europarl.europa.eu/
18. https://www.foreignaffairs.com/
19. https://www.hybridcoe.fi/
20. https://www.kas.de/
21. https://www.oecd-ilibrary.org/
22. https://www.routledge.com
23. https://www2.deloitte.com/us/

Iulian DINULESCU
University of Craiova, Romania

BETWEEN THE SACRED AND THE VIOLENT: THE RUSSIAN IMPERIAL MOVEMENT AND THE NEW PARADIGM OF TERRORISM

Abstract:	*The Russian Imperial Movement (RIM) is an ultra-nationalist and extremist organization that combines imperialist ideology with a rigid view of Russian Orthodoxy. The RIM's distinctive feature is the use of religious symbolism to legitimize both its political goals and violent actions, including involvement in armed conflict and acts of terrorism. The group is known for providing paramilitary training to far-right extremists in Europe, contributing to violent attacks such as the Sweden bombings.* *Although designated a terrorist organization by the United States, Canada, Australia, and the European Union, RIM continues to operate relatively freely in Russia, gaining influence through propaganda and recruitment activities. The movement advocates a vision of Russia as a pure Orthodox nation engaged in a sacred confrontation against what it perceives as decadent and demonic Western values.* *This article explores the dynamics between religion, nationalism, and political violence within RIM, showing how Orthodox symbolism is instrumentalized to support an extremist agenda. RIM is not only a political movement, but also an ideological force that combines religious radicalism with imperialist goals, generating significant global security risks through collaboration with other extremist groups and by disseminating its messages through social media.*
Keywords:	**Religion; symbolism; extremism; Russian imperial movement; ideology; terrorism**
Contact details of the authors:	E-mail: iuliandinulescu@gmail.com
Institutional affiliation of the authors:	**Doctoral School of Orthodox Theology "Saint Nicodim", University of Craiova, Romania**
Institutions address:	Al. I. Cuza Street, 13, Craiova, 200585, phone: 0251 419 900; www.ucv.ro

Introduction

The Russian Imperial Movement (RIM) was designated as a global terrorist organization by the U.S. Department of State on April 6, 2020, making it the first white supremacist organization to receive this classification[1]. RIM and its leaders, Stanislav Vorobiev, Denis Gariyev, and Nikolay Trushchalov, were labeled as global terrorists due to their provision of paramilitary training and their connections to terrorist attacks in Europe, including in Sweden. This designation freezes their assets in the U.S. and prohibits financial transactions, strengthening international counterterrorism measures[2]. The designation was based on RIM's paramilitary activities and involvement in extreme violence, including support for conflicts in Ukraine and

[1] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[2] Michael R. Pompeo, *United States Designates Russian Imperial Movement and Leaders as Global Terrorists* - Press Statement, April 7, 2020, https://2017-2021.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/ (20.09.2024)

participation in terrorist attacks across Europe[1]. RIM's classification as a global terrorist organization marked a significant step in combating the influence of this movement[2].

This designation allows Western governments to impose financial sanctions on RIM members and take legal action against those collaborating with the movement. However, RIM leaders claimed that this label has increased the organization's popularity, aiding in the recruitment of new members[3]. Similarly, the Australian government-imposed sanctions on RIM on May 18, 2022, on charges of financing terrorism under the United Nations Charter Act of 1945[4]. Likewise, Belgium sanctioned RIM for terrorism on March 28, 2024; Canada listed it as a terrorist organization on April 20, 2023; Switzerland imposed sanctions on August 23, 2024; the European Union on March 28, 2024; France on April 20, 2023; and Monaco on August 14, 2024[5].

Founded in 2002 in Sankt Petersburg by Vorobyev, RIM established its paramilitary division, the Russian Imperial Legion (RIL), in 2010, led by Denis Gariev, who coordinates all missions and military training sessions[6]. Initially, RIM did not have a significant influence, with its primary goal being the restoration of the monarchy in Russia and the revival of the Russian Empire[7]. RIM has trained foreign fighters and members of extremist groups or organizations at its training camps in Sankt Petersburg. These fighters were involved in terrorist attacks, including in Sweden, where members of the Nordic Resistance Movement (NRM) carried out bomb attacks in 2016 and 2017 after receiving training from RIM[8]. These actions contributed to justifying RIM's designation as a global terrorist organization[9]. Swedish extremists trained by RIM carried out attacks on migrant centers and a café[10]. Thus, the Russian Imperial Movement (RIM) was designated as a global terrorist organization by the U.S. in 2020 due to its involvement in terrorist attacks and its training of European extremists. The designation freezes financial assets and allows for international sanctions but has also boosted the group's popularity, facilitating the recruitment of new extremist members.

The religious and nationalist ideology of RIM

RIM identifies as a nationalist far-right group with a strong religious component rooted in Russian Orthodoxy. The group promotes a conservative vision that merges Orthodox Christianity with ultra-nationalist and imperialist ideologies. Their religiosity is central to their justification of a vision for the revival of the Russian Empire, believing that Russian Orthodoxy must play a crucial role in restoring monarchical order and a Russia that is ethnically and religiously "pure"[11]. The organization promotes the idea that imperial power,

---

[1] Mapping Militant Organizations, *Russian Imperial Movement*, last modified April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[2] Taylor Chin, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, CTEC – The Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies, Occasional paper, June 2024, pp. 9-10, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1 (25.09.2024)

[3] *Ibidem*, pp. 10-13

[4] Parliament of Australia, *Russian Imperial Movement – Petition*, 12 February 2024, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F27600%2F0136%22 (02.10.2024)

[5] Open Sanctions, *Russian Imperial Movement - Terrorism · Sanctioned entity*, https://www.opensanctions.org/entities/NK-ARaHWXZ8AFcGWX7qnSyd6o/ (20.10.2024)

[6] Taylor Chin, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, CTEC – The Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies, Occasional paper, June 2024, p. 6, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1 (25.09.2024)

[7] Anna Kruglova, *The Russian Imperial Movement, the war in Ukraine and the future of Russian state*, 01 Sep 2023, https://www.icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state (06.09.2024)

[8] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[9] *Idem*

[10] Michael R. Pompeo, Secretary of State, *United States Designates Russian Imperial Movement and Leaders as Global Terrorists* - Press Statement, April 7, 2020, https://2017-2021.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/ (20.09.2024)

[11] Daveed Gartenstein-Ross, Emelie Chace-Donahue, Colin P. Clarke, *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 25 Jan 2023, https://www.icct.nl/publication/understanding-us-designation-wagner-group-transnational-criminal-organisation (06.09.2024)

supported by Orthodoxy, represents the ideal form of governance. This view is tied to a "belief in the divine right of kings", emphasizing a return to the Tsarist political structure of Russia[1]. RIM grounds its ideology in a combination of Russian extreme nationalism and Russian Orthodoxy, perceived as the core of the ethnic and cultural identity of the Russian people[2]. Orthodoxy is employed to legitimize not only their political agenda but also the violence used to achieve these objectives[3]. RIM members adhere to a strict structure, maintaining a dualistic vision in which they are to belong to the "Russian Orthodox Church" and support the establishment of "a Russian imperial state"[4].

RIM does not simply promote Orthodox religion but a specific view of Christianity that closely links Russian identity to Orthodox faith. This perspective is explicit in many of the group's messages, which criticize what they perceive as the moral decay of modern Russia due to its distancing from religion and genuine spiritual traditions[5]. RIM asserts that the Russian people suffer from a lack of faith and that this spiritual crisis is the reason the nation faces both external and internal threats. They also present themselves as a devout religious minority, preserving the purity of Orthodox life and willing to fight to protect Russian Christianity from perceived enemies, both internal and external[6]. Therefore, Orthodox religion is used, in a distorted way, both as a cultural symbol and as a tool to legitimize the organization's political and military objectives. In practice, it is a revival of Russian national identity through Orthodox faith, viewed as a unifying factor among Russian populations within territories claimed by Russia[7]. Messianic nationalism and religion are tightly intertwined in RIM's ideology, promoting a millenarian and "eschatological view of politics"[8]. According to this view, people are living in the end times, with globalism seen as the work of the Antichrist, Islamism as a demonic force, and the Covid-19 pandemic as a strategy by globalists to consolidate the Antichrist's rule[9]. This religious rhetoric serves as an ideological foundation for many of RIM's violent actions, including its participation in armed conflicts, such as in Ukraine. Using the notion of defending Christian values, RIM justifies the use of force to protect its ideals and support what it considers a holy struggle against the West and liberal influences, which, according to the group, endanger Orthodox faith and Russian traditions[10]. RIM also perceives itself as persecuted for its beliefs, viewing its actions as a form of modern martyrdom in the name of Russian Orthodoxy and a restored monarchy[11]. Thus, the group's religiosity is not only a cultural component but an integral part of its nationalist and extremist ideology, justifying radical and violent actions[12]. RIM's ideology is anchored in an extreme anti-liberal stance[13] and relies on a

[1] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, "CTC SENTINEL, Combating Terrorism Center at West Point", August 2023, Vol. 16, No. 8, p. 26, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[2] Mapping Militant Organizations, *Russian Imperial Movement*, last modified April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[3] Taylor Chin, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, CTEC – The Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies, Occasional paper, June 2024, p. 6, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1 (25.09.2024)

[4] The Cipher Brief, *Russian Imperial Movement Labeled a Specially Designated Global Terrorist Entity*, April 7th, 2020, https://www.thecipherbrief.com/column_article/russian-imperial-movement-labeled-a-specially-designated-global-terrorist-entity (20.10.2024)

[5] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[6] *Idem*

[7] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, in CTC SENTINEL, Combating Terrorism Center at West Point, August 2023, Vol. 16, No. 8, p. 23, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[8] Nicolas Lebourg, Olivier Schmitt, *The French ultra-right's attraction to Putin's Russia*, University de Montpellier, published on September 25, 2024, https://www.umontpellier.fr/en/articles/lattirance-de-lultra-droite-francaise-pour-la-russie-de-poutine (20.10.2024)

[9] *Idem*

[10] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[11] *Idem*

[12] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

combination of Russian nationalism, Orthodoxy, and anti-Semitism, all supporting the restoration of the Russian Empire and vehemently opposing foreign influences, particularly those from the West[1]. Therefore, Orthodox religion is central to legitimizing the group's ultra-reactionary and nationalist ideology. RIM views Orthodoxy as the foundation of Russian national identity and a tool to justify violent actions, presenting the restoration of the Russian Empire as a "sacred mission".

The role of the religious symbolism in mobilizing supporters

RIM uses Orthodox and imperial symbols to legitimize its ideology. It associates religious symbols like the Orthodox cross with nationalist messages, claiming that the restoration of the Russian Empire is a sacred mission, justified by both Orthodox faith and Russia's monarchical history[2]. This combination of religious symbolism and nationalism is part of their strategy for mobilizing and recruiting followers, reinforcing the idea that their struggle is divinely sanctioned[3]. Religious symbolism plays a central role in RIM's propaganda and public image. The group frequently uses Orthodox symbols, such as the cross and other religious imagery, in combination with monarchical symbols to create a narrative where Orthodox Russia and the pre-1917 Russian Empire are portrayed as eras of national glory and purity[4]. This mix of symbols reinforces RIM's message that the restoration of the Russian Empire is not only a political goal but also a sacred duty, religiously justified[5]. Religious symbolism is frequently employed by RIM to justify both its military actions and its political vision.

The organization presents itself as a defender of Orthodox values in the face of modernism, liberalism, and multiculturalism, promoting a militant version of Orthodoxy. RIM members see the war in Ukraine as an opportunity to protect Orthodox faith and expand the borders of "New Russia," a concept that includes eastern and southern Ukraine[6]. RIM appeals to a strong religious symbolism rooted in Russian Orthodoxy to lend legitimacy to its nationalist ideology and violent actions[7]. The group projects the idea that Russia is the only "pure" Orthodox nation, called to save traditional Christian values from the "decadent" influences of the West[8]. Russian Orthodoxy is presented not merely as a religion but as an essential component of national identity, thus shaping a narrative of "holy war" where violence is justified as a necessary means of defending the faith. This religious narrative aids in mobilizing supporters both inside and outside of Russia, giving them a sense of divine mission[9]. The Orthodox cross and other religious symbols are used as elements of legitimacy, invoking a direct connection between Orthodox tradition and the Russian monarchy. RIM views these symbols as part of the "natural" identity of the Russian people, in opposition to the "foreign" values brought by liberalism, democracy, and secularism[10]. These religious symbols are often used in protests and demonstrations alongside images of the last Tsar of Russia, Nicholas II, whom RIM views as a religious martyr for the Russian

---

[13] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, "CTC SENTINEL, Combating Terrorism Center at West Point", August 2023, Vol. 16, No. 8, p. 24, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[1] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[2] Daveed Gartenstein-Ross, Emelie Chace-Donahue, Colin P. Clarke, *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 25 Jan 2023, https://www.icct.nl/publication/understanding-us-designation-wagner-group-transnational-criminal-organisation (06.09.2024)

[3] *Idem*

[4] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[5] *Idem*

[6] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, in CTC SENTINEL, Combating Terrorism Center at West Point, August 2023, Volume 16, Issue 8, p. 23, p. 25, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[7] Daniel J. White, Jr., *Vanguard of a White Empire: Rusich, the Russian Imperial Movement, and Russia's War of Terror*, Naval Postgraduate School (U.S.), Center for Homeland Defense and Security, Monterey, California, USA, March 2024, p. 14, https://www.hsdl.org/c/abstract/?docid=881387 (20.10.2024)

[8] *Ibidem*, p. 17

[9] *Ibidem*, pp. 71-73

[10] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

nation[1]. Imperial and Orthodox symbols are essential in their propaganda messages, being used to create a link between the present and the glorious past of Orthodox Russia[2]. Moreover, RIM's religious symbolism includes references to biblical elements, used to denounce behaviors and values the group considers "immoral" or "decadent"[3]. For instance, RIM uses the story of Sodom and Gomorrah to condemn decadence and other behaviors it deems deviant, describing them as condemned by God and destructive to Russian society[4].

Religious symbolism, combined with nationalist and imperial symbols, helps create a group identity for RIM members, who see themselves not only as political activists but as soldiers for a divine cause, defenders of Orthodox faith and Russian ethnic identity[5]. This use of sacred symbols gives RIM members a sense of mission that goes beyond mere politics, transforming their violent actions into a form of "modern crusade" for national rebirth[6]. RIM uses Russian Orthodox symbols and other religious imagery to justify violence, blending spiritual traditions with nationalism. These symbols legitimize far-right extremist ideology and attract supporters through a distorted religious mythology that promotes sacrifice and struggle against the perceived "enemy". Thus, religion becomes a strategic tool for mobilization and online recruitment[7]. "Approximately 40% of posts" by movement members "on social media" include religious themes. These references are often linked to the idea that Russia must return to a "natural" state and restore the monarchy, presented as a God-given order[8]. Additionally, RIM associates many of Russia's modern problems with the abandonment of Orthodox religion and the "assassination of the last Tsar", seen as a "curse" upon the nation[9]. Their symbolic messages thus frequently include religious iconography and descriptions of their fighters, depicted as "Knights of Christ" and "martyrs"[10].

RIM's propaganda is highly active online, using social networks such as VKontakte to spread nationalist messages and recruit members[11]. The messages include narratives of authenticity and legitimacy, presenting the group as a defender of Russian traditions and a guarantor of "true values". RIM also portrays itself as an organization that understands the concerns and grievances of the public, thus building an emotional connection with its audience[12]. Through social media and other media channels, RIM aggressively propagates its ideology, portraying Russia as a "holy nation" that must save the West from what it considers to be moral decay. This propaganda is effective in mobilizing supporters and recruiting new members, who join the movement believing they are part of a divine mission to save civilization[13]. Thus, religious symbolism, combined with imperialistic and anti-liberal ideas, transforms the political struggle into a perceived divine one. Religion thus becomes a tool for mobilization, offering justification for the group's radical goals and extremist actions.

---

[1] *Idem*

[2] Taylor Chin, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, CTEC – The Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies, Occasional paper, June 2024, p. 6, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1 (25.09.2024)

[3] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[4] *Idem*

[5] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[6] *Idem*

[7] Sara Morrell, *Mapping Extremist Discourse Communities on Telegram: The Case of the Russian Imperial Movement*, "Global Network on Extremism&Technology", 18th of September 2023, https://gnet-research.org/2023/09/18/mapping-extremist-discourse-communities-on-telegram-the-case-of-the-russian-imperial-movement/ (30.09.2024)

[8] Anna Kruglova, *For God, for Tsar and for the Nation: Authenticity in the Russian Imperial Movement's Propaganda*, in Studies in Conflict & Terrorism, Vol. 47, No. 6, 2024, pp. 652-654, https://doi.org/10.1080/1057610X.2021.1990826 (30.09.2024)

[9] *Ibidem*, pp. 652-654

[10] *Ibidem*, pp. 656-657

[11] *Ibidem*, pp. 649

[12] *Ibidem*, pp. 654-656

[13] Daniel J. White, Jr., *Vanguard of a White Empire: Rusich, the Russian Imperial Movement, and Russia's War of Terror*, Naval Postgraduate School (U.S.), Center for Homeland Defense and Security, Monterey, California, USA, March 2024, pp. 36-40, https://www.hsdl.org/c/abstract/?docid=881387 (20.10.2024)

RIM and the international extremist networks

RIM maintains strong ties with other far-right extremist groups within Russia and abroad, including neo-Nazi groups. Although RIM does not officially define itself as a neo-Nazi organization, many of its members share similar extremist beliefs, including antisemitism and xenophobia towards immigrants[1]. RIM's extremism is not limited to regional conflicts; it has a global dimension. The group actively seeks connections with other supremacist and extremist organizations in Europe and the USA, playing a significant role in the transnational white supremacist movement[2]. RIM organizes military training sessions for extremists from other countries and participates in international conferences with other far-right groups, helping expand cooperation networks among these organizations[3]. RIM stands out for its international alliances with extremist groups, such as the NRM and US-based supremacist groups. These collaborations facilitate the exchange of ideologies, propaganda, and paramilitary training. Partizan, RIM's paramilitary wing, provides training not only for its members but also for other extremist groups, strengthening global networks of radicalization[4]. RIM has become a central pillar of far-right extremism in Russia and Europe, actively supporting terrorist attacks and providing paramilitary training to extremists worldwide[5]. The training provided at its camps in St. Petersburg reflects its ties to other international extremist groups, such as NRM, Germany's National Democratic Party, and U.S.-based organizations like the Traditionalist Worker Party (TWP), which provides logistical and material support[6]. RIM has also trained the youth wing of the German neo-Nazi group The Third Path in advanced military tactics[7]. RIM has been accused of engaging in terrorist attacks, including the 2022 bombings in Spain, where letter bombs were sent to embassies and official residences[8]. Between November and December 2022, RIM was accused of involvement in sending six letter bombs in Spain, including to the residence of the Spanish Prime Minister and the USA and Ukrainian embassies[9]. These attacks demonstrate that RIM is not limited to extremist propaganda but has both the capability and intent to conduct violent attacks outside Russia, amplifying its international security risk[10].

RIM leader Stanislav Vorobiev acknowledged in an interview in early February 2023 that the movement has sympathizers in the United States, Spain, New Zealand, and Australia, and recruits new members, including for its military wing, through social media accounts[11]. RIM has provided financial assistance to NRM, indicating a partnership beyond shared ideologies, and a RIM leader spoke at "Nordic Days" in 2015, an event hosted by NRM, revealing some level of cooperation or ideological alignment

[1] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, "CTC SENTINEL, Combating Terrorism Center at West Point", August 2023, Vol. 16, No. 8, p. 24, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[2] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[3] *Idem*

[4] Talya Ackerman, *The Russian Imperial Movement: Digital Crusades and Orthodox Christian Supremacy*, "GARNET - Global Affairs and Religion Network", April 19, 2024, Student Events, https://garnet.elliott.gwu.edu/2024/04/19/february-2-2024-the-russian-imperial-movement-digital-crusades-and-orthodox-christian-supremacy-by-talya-ackerman/ (30.09.2024)

[5] Daniel J. White, Jr., *Vanguard of a White Empire: Rusich, the Russian Imperial Movement, and Russia's War of Terror*, Naval Postgraduate School (U.S.). Center for Homeland Defense and Security, Monterey, California, USA, March 2024, pp. 42-43, https://www.hsdl.org/c/abstract/?docid=881387 (20.10.2024)

[6] Anna Kruglova, *For God, for Tsar and for the Nation: Authenticity in the Russian Imperial Movement's Propaganda*, "Studies in Conflict&Terrorism", Vol. 47, No. 6, 2024, pp. 648-649, https://doi.org/10.1080/1057610X.2021.1990826 (20.10.2024)

[7] Counter Extremism Project, *Russian Imperial Movement Provides Weapons & Combat Training to German Neo-Nazis*, June 11, 2020, https://www.counterextremism.com/press/russian-imperial-movement-provides-weapons-combat-training-german-neo-nazis (20.10.2024)

[8] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[9] *Idem*

[10] Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/ (06.09.2024)

[11] Mark Greenblatt, *Russian Imperial Movement linked to terror campaign in Europe*, "Scripps News", Feb 10, 2023, https://www.scrippsnews.com/world/europe/russian-imperial-movement-linked-to-europe-terror-campaign (20.10.2024)

between the two groups[1]. In September 2017, a RIM representative spent an extended period in the United States "connecting" with TWP, another far-right, national-socialist organization[2]. TWP was active in promoting white supremacy and antisemitic ideologies before disbanding in 2018 due to legal challenges and internal conflicts. Closely allied with other white supremacist organizations, TWP was involved in the violent Charlottesville protest in 2017[3]. One of TWP's founders, Matthew Heimbach, became associated with the "alt-right". Heimbach is described as "a virulent antisemite" who promotes an extreme version of Orthodoxy to support "white nationalist views". He believes that "traditional religion is crucial to preserving white heritage and culture" and sees it as "a bulwark against secular humanism, multiculturalism, and globalism"[4].

In 2014, Matthew Heimbach "was publicly rebuked by the priest at his Orthodox Christian church, who said that Heimbach "must cease and desist all activities…promoting racist and separationist ideologies"[5]. Heimbach met with RIM members in the United States in September 2017, expressing TWP's desire to serve as a representative for America at future RIM-organized gatherings. According to Heimbach, his ties with RIM date back to 2015. Heimbach played a central role in organizing the Unite the Right protest in Charlottesville in August 2017, where a car attack by a white supremacist caused one death and injured many others[6]. Following academic research, Iulian Dinulescu concluded that neo-legionary religious fanaticism, based on the ideology of the Archangel Michael Legion in Romania, known as the Iron Guard, remains relevant through a combination of ultra-nationalist, religious, and antisemitic ideas. Research revealed that Matthew Heimbach, an American extremist, considers Corneliu Zelea Codreanu an inspiration. During the violent protests in Charlottesville on August 12, 2017, Heimbach appeared wearing a shirt with Codreanu's image, expressing admiration for the legionary leader. This event, which included violence resulting in deaths and injuries, demonstrated the influence of Romanian neo-legionary ideology on the American far-right, confirmed by experts such as Radu Ioanid[7].

RIM is also involved in cooperation with other neo-Nazi groups, including Rusich and the Wagner Group[8]. Despite its connections with international extremist groups, RIM's stance toward the Russian government remains ambiguous, allowing it to remain active without severe repression[9]. RIM actively engages with the global community, striving to broaden its worldwide impact. The movement partners with various extremist factions, including white supremacist groups across Europe and the United States, to propagate its aggressive ideology[10]. By April 2024, RIM had "over 50,000 followers online"[11]. Since 2015, RIM has expanded its international networks by creating a World National-Conservative Movement in collaboration

---

[1] Lucas Webber, Alec Bertina, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, "CTC SENTINEL, Combating Terrorism Center at West Point", August 2023, Vol. 16, No. 8, p. 24, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/ (09.09.2024)

[2] *Ibidem*, p. 24

[3] SPLC, *Traditionalist Worker Party*, "The Southern Poverty Law Center", https://www.splcenter.org/fighting-hate/extremist-files/group/traditionalist-worker-party (12.09.2024)

[4] *Matthew Heimbach: Five Things to Know*, "Anti-Defamation League" May 01, 2018, https://www.adl.org/resources/news/matthew-heimbach-five-things-know (12.09.2024)

[5] *Idem*

[6] Counter Extremism Project, *Russian Imperial Movement Provides Weapons&Combat Training To German Neo-Nazis*, June 11, 2020, https://www.counterextremism.com/press/russian-imperial-movement-provides-weapons-combat-training-german-neo-nazis (20.10.2024)

[7] Iulian Dinulescu, *Fanatismul religios legionar: de la apariţia în România la promovarea de către extrema dreaptă din Statele Unite ale Americii*, Top Form, 2020, pp. 127-128

[8] Anna Kruglova, *The Russian Imperial Movement, the war in Ukraine and the future of Russian state*, 01 Sep 2023, https://www.icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state (06.09.2024)

[9] Daveed Gartenstein-Ross, Emelie Chace-Donahue, Colin P. Clarke, *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 25 Jan 2023, https://www.icct.nl/publication/understanding-us-designation-wagner-group-transnational-criminal-organisation (06.09.2024)

[10] Taylor Chin, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, CTEC – The Center on Terrorism, Extremism and Counterterrorism, Middlebury Institute of International Studies, Occasional paper, June 2024, p. 18, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1 (25.09.2024)

[11] Ethan Ingram, *Stopping Online Terrorism: Pulling the Plug on the Russian Imperial Movement*, "The International Affairs Review", https://www.iar-gwu.org/blog/iar-web/stopping-online-terrorism (30.09.2024)

with Rodina ("Motherland") - the far-right Russian party. The organization does not exclusively focus on "defending the white race or Christians," but extends invitations to 58 groups worldwide, including countries such as Thailand, Japan, Syria, and Mongolia, as well as the United States[1]. RIM is not an isolated entity but part of an expanding global network of white nationalist groups. These groups collaborate to produce propaganda, recruit new members, and share paramilitary skills[2]. Thus, RIM collaborates with international extremist groups, consolidating transnational terrorism networks and facilitating the exchange of ultranationalist ideologies. Through military training and online propaganda, it recruits global members and supports violent attacks. The organization, allied with other neo-Nazi groups, poses a global threat to international security.

Conclusions

RIM represents a complex phenomenon of political and religious extremism that combines Russian nationalism, Orthodox religiosity, and paramilitary violence to achieve its objectives. Although founded on the ideology of restoring the Russian Empire, RIM has evolved into a transnational movement capable of destabilizing multiple regions, both through direct actions and by collaborating with other far-right extremist groups and organizations across Europe and the USA. A distinctive feature of RIM is its use of Orthodox religious symbolism to justify violence. The group instrumentalizes Russian Orthodoxy not only to legitimize its political agenda but also to mobilize public support. By crafting an eschatological narrative that portrays Russia as the ultimate defender of Christian values against the "decadent" West, RIM forges a link between national and religious identity, offering its supporters a sense of divine mission. This narrative leads to a progressive radicalization of its followers, transforming them into "soldiers of faith", ready to use violence to defend Orthodoxy and Russia from perceived internal and external threats. Thus, religion becomes not merely an ideological framework but a catalyst for violent action, justifying terrorism and armed conflicts. Religious concepts are manipulated to turn political struggle into a modern "crusade" against globalism and liberalism, with a focus on Russian national and ethnic values.

Internationally, RIM has transformed these ideas into a mechanism for global mobilization, recruiting extremists from various countries and providing them with military training and logistical support. Thus, RIM has managed to create a transnational network that extends beyond mere ideology to become a functional infrastructure for terrorism. Its network of collaborators includes neo-Nazi groups, white supremacist movements, and other far-right organizations, such as the Nordic Resistance Movement (NRM) and the Traditionalist Worker Party (TWP) in the USA. Active involvement in international conflicts, like the one in Ukraine, demonstrates how RIM exploits regional instability to advance its own goals. Recruiting volunteers for combat and expanding its influence in other war zones, such as Syria and Libya, reflects the group's global ambitions. Furthermore, its involvement in terrorist attacks, like those in Sweden and Spain, shows that RIM is capable of inciting violence not only in Russia but on other continents as well. Another important dimension of RIM's strategy is its use of social media platforms for propaganda, recruitment, and coordination of violent actions. Through networks like VKontakte and Telegram, the group spreads messages of hate, promotes the superiority of Russian nationalism, and attracts new recruits from around the world. Notably, RIM not only disseminates its extremist ideology online but also organizes paramilitary courses for extremists, strengthening its global networks of radicalization. Despite being sanctioned and labeled a terrorist organization by numerous states and international bodies, RIM persists in its activities under the lenient oversight of the Russian government. This ambiguity in its position relative to the Russian state allows it to expand its influence and act within a "gray area" between national legality and transnational terrorism.

In conclusion, RIM is not merely a political or religious movement, but an extremely dangerous phenomenon that combines religion, nationalism, and terrorist violence into a form of globalized extremism. With its ability to mobilize supporters internationally, forge alliances with other extremist groups, and use modern technology for propaganda and recruitment, RIM poses a major threat to global security.

---

[1] Nicolas Lebourg, Oliver Schmitt, *The French ultra-right's attraction to Putin's Russia*, University de Montpellier, September 25, 2024, https://www.umontpellier.fr/en/articles/lattirance-de-lultra-droite-francaise-pour-la-russie-de-poutine (20.10.2024)

[2] Mark Greenblatt, *Inside the Global Fight for White Power*, July 23, 2022, "Reveal", https://revealnews.org/podcast/inside-global-fight-for-white-power/ (20.10.2024)

Bibliography

Books

1. Dinulescu, Iulian, *Fanatismul religios legionar: de la apariţia în România la promovarea de către extrema dreaptă din Statele Unite ale Americii*, Top Form, București, 2020

Articles and Studies

1. Ackerman, Talya, *The Russian Imperial Movement: Digital Crusades and Orthodox Christian Supremacy*, "Garnet. Global Affairs and Religion Network", April 19, 2024, https://garnet.elliott.gwu.edu/2024/04/19/february-2-2024-the-russian-imperial-movement-digital-crusades-and-orthodox-christian-supremacy-by-talya-ackerman/
2. Chin, Taylor, *The Justification for Designating the Russian Imperial Movement as a Foreign Terrorist Organization*, "CTEC – The Center on Terrorism, Extremism and Counterterrorism", Middlebury Institute of International Studies, June 2024, https://drive.google.com/file/d/11bPEu7bg5Xf0osF1xOthBQ9DASIAq1Gz/view?pli=1
3. Ingram, Ethan, *Stopping Online Terrorism: Pulling the Plug on the Russian Imperial Movement*, "The International Affairs Review", https://www.iar-gwu.org/blog/iar-web/stopping-online-terrorism
4. Kruglova, Anna, *For God, for Tsar and for the Nation: Authenticity in the Russian Imperial Movement's Propaganda*, "Studies in Conflict&Terrorism", Vol. 47, No. 6, 2024, https://doi.org/10.1080/1057610X.2021.1990826
5. *Matthew Heimbach: Five Things to Know*, "Anti-Defamation League" May 01, 2018, https://www.adl.org/resources/news/matthew-heimbach-five-things-know
6. Morrell, Sara, *Mapping Extremist Discourse Communities on Telegram: The Case of the Russian Imperial Movement*, "Global Network on Extremism&Technology", September 2023, https://gnet-research.org/2023/09/18/mapping-extremist-discourse-communities-on-telegram-the-case-of-the-russian-imperial-movement/
7. Webber, Lucas; Bertina, Alec, *The Russian Imperial Movement in the Ukraine Wars: 2014-2023*, "CTC SENTINEL, Combating Terrorism Center at West Point", August 2023, Vol. 16, No. 8, https://ctc.westpoint.edu/the-russian-imperial-movement-in-the-ukraine-wars-2014-2023/
8. White, Daniel J., Jr., *Vanguard of a White Empire: Rusich, the Russian Imperial Movement, and Russia's War of Terror*, Naval Postgraduate School (U.S.). Center for Homeland Defense and Security, Monterey, California, USA, March 2024, https://www.hsdl.org/c/abstract/?docid=881387

Documents

1. Mapping Militant Organizations, *Russian Imperial Movement*, April 7, 2023, https://mappingmilitants.org/node/513/
2. Open Sanctions, *Russian Imperial Movement - Terrorism · Sanctioned entity*, https://www.opensanctions.org/entities/NK-RaHWXZ8AFcGWX7qnSyd6o/
3. Parliament of Australia, *Russian Imperial Movement Petition*, 12 February 2024, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F27600%2F0136%22

Press articles/Reviews

1. Counter Extremism Project, *Russian Imperial Movement Provides Weapons & Combat Training to German Neo-Nazis*, June 11, 2020, https://www.counterextremism.com/press/russian-imperial-movement-provides-weapons-combat-training-german-neo-nazis
2. Gartenstein-Ross, Daveed, Emelie Chace-Donahue, Colin P. Clarke, *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 25 Jan 2023, https://www.icct.nl/publication/understanding-us-designation-wagner-group-transnational-criminal-organisation
3. Greenblatt, Mark, *Inside the Global Fight for White Power*, July 23, 2022, "Reveal", https://revealnews.org/podcast/inside-global-fight-for-white-power/

4. Greenblatt, Mark, *Russian Imperial Movement linked to terror campaign in Europe*, "Scripps News", February 10, 2023, https://www.scrippsnews.com/world/europe/russian-imperial-movement-linked-to-europe-terror-campaign
5. Kruglova, Anna, *The Russian Imperial Movement, the war in Ukraine and the future of Russian state*, 01 September 2023, https://www.icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state
6. Lebourg, Nicolas, Olivier Schmitt, *The French ultra-right's attraction to Putin's Russia*, University de Montpellier, September 25, 2024, https://www.umontpellier.fr/en/articles/lattirance-de-lultra-droite-francaise-pour-la-russie-de-poutine
7. Pompeo, Michael R., *United States Designates Russian Imperial Movement and Leaders as Global Terrorists* - Press Statement, April 7, 2020, https://2017-2021.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/
8. SPLC, *Traditionalist Worker Party*, "The Southern Poverty Law Center" - Website, https://www.splcenter.org/fighting-hate/extremist-files/group/traditionalist-worker-party
9. The Cipher Brief, *Russian Imperial Movement Labeled a Specially Designated Global Terrorist Entity*, April 7th, 2020, https://www.thecipherbrief.com/column_article/russian-imperial-movement-labeled-a-specially-designated-global-terrorist-entity

Internet sources

1. https://2017-2021.state.gov/
2. https://garnet.elliott.gwu.edu/
3. https://gnet-research.org/
4. https://parlinfo.aph.gov.au/
5. https://revealnews.org/
6. https://www.adl.org/
7. https://www.counterextremism.com/
8. https://www.hsdl.org/
9. https://www.iar-gwu.org/
10. https://www.icct.nl/
11. https://www.scrippsnews.com/
12. https://www.thecipherbrief.com/
13. https://www.umontpellier.fr/

Meljana BREGU
University of Tirana, Albania

ADDRESSING ENVIRONMENT AND CLIMATE CHANGE IN ALBANIA IN THE FRAMEWORK OF THE EU INTEGRATION

Abstract:	*Albania is an EU candidate country that, in the framework of the integration process, is trying to align its policies within the EU's framework of the Green Agenda part of the European Green Deal. Albania has been part of the European Green Agenda for the Western Balkans since 2020, which enhances the goals of the European Green Deal. This Agenda promotes sustainability, green economy initiatives, and decarbonization in line with the EU's environmental and climate goals. Addressing climate change issues by strengthening green transition policies constitutes a fundamental priority for economic integration within the region and with the European Union.* *In this context, Albania has adopted the national climate change strategy, which is compatible with the goals of the European Union's climate and energy package, specifically the National Strategy for Climate Change and Action Plan (NSCCAC) 2020-2030. This policy prioritizes climate change mitigation, adaptation, a clean environment, and clean energy, following EU goals.* *While the country is progressing toward alignment with EU climate goals and policies, has adopted numerous strategies and plans, and has a sound legislative framework, it still lacks the implementation of the legal framework due to national and regional challenges.* *The paper analyzes the challenges and obstacles of implementing the national and European legal framework and EU directives.* *Methodologically, we will analyze and compare progress reports, public speeches, declarations, and national integration strategies.*
Keywords:	**Green Agenda; EU-Integration; environment; climate change**
Contact details of the authors:	E-mail: meljana.bregu@unitir.edu.al
Institutional affiliation of the authors:	**Faculty of History and Philology, University of Tirana, Albania**
Institutions address:	Rr. Elbasanit, Tiranë, Tel.: +3554 22369987 E -mail: fhf@fhf.edu.al Website: fhf.edu.al

Introduction

Since the demise of the communist regime, Albania's principal foreign policy priority has been EU integration. Political forces and the public, who are pro-European Union, support this goal. The integration process has been the primary driving force behind Albania's political, social, and economic reforms. In 2020, Albania advanced its integration process by joining the Green Agenda for the Western Balkans, a regional strategy that aligns with the European Green Deal. This Agenda connects the region to the EU's goal of making Europe carbon neutral by 2050, and it has garnered significant support and encouragement throughout the Balkan region. The Sofia Summit embraced the Agenda in 2020, while the Brdo Summit endorsed the Action Plan in 2021. The aims are divided into five major areas: more clean energy sources to avert climate change, a circular economy, depolluted water, air, and soil, sustainable agriculture, and biodiversity and ecosystem protection[1].

[1] Regional Cooperation Council, *Green Agenda*, 2020, https://www.rcc.int/greenagenda (08.11.2024)

The Green Agenda brings challenges and benefits to the region, but successful implementation requires better cooperation among countries of the region to overcome problems that can't be resolved on a national level[1]. The Regional Cooperation Council (RCC) has played an active role in implementing the Green Agenda and has tried to focus the government, media, and non-governmental organizations on the green transition. The RCC facilitates coordination and communication between Western Balkan countries, backing them in aligning their environmental policies, enhancing expertise, sharing best practices, and working collectively toward sustainable goals. Through initiatives like the Green Agenda, the RCC helps establish a unified approach to addressing environmental issues, setting shared goals, and securing regional stability and prosperity in line with EU standards[2].

Due to the main findings of the Balkan Barometer in 2024, the citizens in the region are mainly concerned about air pollution (57%), water and soil pollution (43%, 38%), extreme weather effects such as floods and earthquakes (32%), poor waste management (37%), and heavy traffic (32%)[3] .The Green Agenda for the Western Balkans can relieve these concerns and contribute to the reduction of pollution of air, water, and soil through the reduction of carbon emissions and can also increase the production of energy from renewable sources that decrease the emissions in the air. The Green Agenda aims to achieve carbon neutrality by 2050, an ambitious goal for all European countries. It poses challenges but also offers opportunities to the region[4]. It can foster cooperation, enhance sustainable development, promote the integration process, promote renewable energy, and improve the quality of life of the region's citizens[5]. The proposed strategy encourages a cooperative approach to climate change, acknowledging the transboundary nature of many challenges and their need for coordinated efforts to achieve practical solutions[6]. These solutions can ensure a friendly environment and address specific problems, such as growing energy costs, which concern 45% of the people in the area[7]. Also, the implementation of the Green Agenda can ensure economic growth, ecological sustainability and social justice like in other region that had benefited from the green transition[8].

The countries are advancing to a green transition through positive actions and are also increasing their renewable energy sectors, like hydropower, solar and wind energy. The countries have used different strategies to ensure more clean energy sources. Serbia is more focused on solar farms to reduce its coal dependence, and Albania and North Macedonia are more involved in wind energy[9].

Despite these efforts, progress has been slow due to the difficulties of increasing energy production from renewable sources in a region that relies entirely on carbon for energy production, except Albania, which uses hydropower plants[10.] This fact has impacted the goal of cleaner energy and is a risk to environmental security since coal contributes significantly to pollution and emissions of greenhouse gases. Abandoning coal as a principal source of energy production may result in social and economic difficulties for many region countries,

---

[1] Sanja Filipovic, Lior Noam, Mirjana Radonavic, *The Green Deal – just transition and sustainable development goals Nexus*, "Renewable and Sustainable Energy Reviews", Vol. 168, No. 13, 2022, p. 2 https://doi.org/10.1016/j.rser.2022.112759 (08.11.2024)

[2] Regional Cooperation Council, https://www.rcc.int/greenagenda (08.11.2024)

[3] Regional Cooperation Council, *Balkan Public Barometer 2024*, https://www.rcc.int/balkanbarometer/results/2/public (08.11.2024)

[4] Miljana Durcevic Cucic, *European Union Practices Turn in "Green" Policies in the Western Balkans Accession Negotiations*, "Science, International Journal", Vol. 3, No. 4. 2024, pp. 181-186

[5] Mirjana Radovic Markovic, D. Jovancevic, Z. Nikitovic, *Toward green economy: opportunities and obstacles for Western Balkan countries*, Xlibris Publishing, Bloomington, 2016, p. 75

[6] Jelena Šogorov-Vučković, Dušan Piksiades, Ivan Trifunović, *Governmental investment in the environmental economy in the Western Balkan*, "The European Journal of Applied Economics", Vol. 19, No. 1, 2022, pp. 121-136, DOI: 10.5937/ejae19-33686 (08.11.2024)

[7] Regional Cooperation Council, *Balkan Public Barometer 2024*, https://www.rcc.int/balkanbarometer/results/2/public (08.11.2024)

[8] David Gibbs, Kirstie O' Neill, *Future Green Economies and Regional Development: a research Agenda*, "Regional Studies", Taylor and Francis, Vol. 15, No. 1, 2017, p. 161

[9] Aspen Institute, *Green Agenda for the Western Balkans*, https://www.aspeninstitute.de/wp-content/uploads/Green-Agenda-for-the-Western-Balkans_2023.pdf (09.11.2024)

[10] Jelena Zvezdanović Lobanova, *The Green Transition and Energy Security in the Western Balkans Countries*, 2024, pp. 544-569, doi:10.18485/iipegsirescu. 2024.ch24 (08.11.2024)

such as increased unemployment due to a drop in the coal sector workforce[1]. For this reason, governing political forces are not inclined toward a rapid green transition. Due to these challenges, and even though the region has a great potential to increase the production of renewable energy, the green transition remains still slow, and the region faces a series of challenges in achieving the target and the goals for renewable energy[2]. Albania and Montenegro were the only countries in the region that accomplished good progress in 2020 due to the increase in energy production from renewable sources, which was 44.5% and 39.5%, respectively[3]. However, these countries' high percentages of renewable energy are also related to biofuels andood used for co oking and heating, especially in the coldest areas but this renewable source of energy is a cause of environmental pollution[4]. The fact that Albania does not rely on carbon for electricity production does not make it less vulnerable; instead, it leads to massive energy imports during periods of low rainfall and, above all, results in an intense exploitation of water resources.

To sustain the region and to facilitate the implementation of the Green Agenda, the EU plays a fundamental role. The European Economic and Investment Plan for the Western Balkans promotes the Green Agenda by increasing investments in sustainable transportation and clean energy. It has allocated a substantial financial package of up to €9 billion in EU funds, potentially mobilizing up to €20 billion of investments through the Western Balkan Guarantee Facility[5]. EU support is necessary in a region that still suffers economic constraints and where governments cannot finance costly projects or sustain the use of renewable energy through incentives in the private sector. The political, national, financial, and regional constraints can impact the green transition in the region, so the EU pressure and sustainment need to be present and comprehensive. The paper will focus on Albania's obstacles in developing sustainable energy sources and implementing a climate change strategy.

Albanian initiatives regarding climate change

The integration in Albania process is endorsed not only by the political forces but also by the public opinion; due to the Balkam Barometer, 77% of the Albanians sustain that the integration would be a positive step for the country[6]. In 2009 the country has signed the Stabilization-Association Agreement, in 2014 Albania was granted the candidate status and in 2020 the Council opened accession negotiations with Albania and Norther Macedonia giving a positive signal for the region integration into the EU[7]. Albania aims to become a full EU member by 2030 fulfilling the requested negotiations conditions.

Albania is trying to pursue the achievement of sustainable development goals and environmental protection conditions according to the Green Agenda for the Western Balkans. Also, in the framework of the integration process has committed to achieve climate neutrality by 2050 and to meet EU directives and to integrate the EU objectives into the legal framework. The government has adopted specific strategies and laws that enhance the regulatory framework on climate change and the environment, driven by the efforts to approximate the EU environmental acquis. Albania has adopted the National Energy Strategy (2018-2030), National Climate Change Strategy (2019), Law on Climate Change, National Action Plan for renewable energy resources in Albania (2019-2021) and is amending the National Climate Strategy and the National Energy Strategy to align with the Green Agenda objectives[8]. The legal framework is in line with the EU priorities, but the problem is the lack of implementation of the legal framework.

---

[1] Jelena Ignjatović, Sanja Filipović, Mirjana Radovanović, *Challenges of the green transition for the recovery of the Western Balkans*, "Energy. Sustainability and Society", 2024, Vol. 14, pp. 1-13, doi: 10.1186/s13705-023-00421-4 (08.11.2024)

[2] Agora Energiewende, *Powering the future of the Western Balkans with Renewables*, https://www.agora-energiewende.org/fileadmin/user_upload/2021-01_EU_Balkan_Green_Deal.pdf (13.11.2024)

[3] Stefan Dunjic, Simon Pezzutto, Alyona Zubaryeva, *Renewable Energy development trends in the Western Balkans*, "Renewable and Sustainable Energy Reviews", Vol. 65, 2016, pp. 1026-1032 https://www.sciencedirect.com/science/article/abs/pii/S1364032116301630?via%3Dihub (13.11.2024)

[4] Aspen Institute, *Green Agenda for the Western Balkans,* https://www.aspeninstitute.de/wp-content/uploads/Green-Agenda-for-the-Western-Balkans_2023.pdf (09.11.2024)

[5] https://www.wbif.eu/ (11.11.2024)

[6] https://www.rcc.int/balkanbarometer/key_findings_2024/2/public (11.11.2024)

[7] https://integrimi-ne-be.punetejashtme.gov.al/anetaresimi-ne-be/historiku/ (14.11.2024)

[8] OECD, *Multi-dimensional Review of the Western Balkans: From Analysis to Action*, OECD Development Pathways, OECD Publishing, Paris, 2022, https://doi.org/10.1787/8824c5db-en (11.11.2024)

The integration process closely links with the transition to a green economy, and the "negotiating framework" includes the Green Agenda. The "negotiating framework" for Albania was presented by the European Council in 2022 and includes guidelines and principles for the accession negotiations regarding Chapter 27 (Environment and Climate Action), which is included in Cluster 4: Green Agenda and Sustainable connectivity which also incorporates transport policy, energy, and trans-European networks[1].

Chapter 27 is considered one of the most expensive in terms of costs, human resources and actors involved; it includes vertical and horizontal legislation and contains provisions addressing climate change[2]. Since 2020, the EU and other donors has pledged to financially endorse and support Albania's implementation of the Green Agenda by providing technical and financial assistance in energy efficiency, renewable energy, and environmental management[3]. The EU with other donors like the Sweden is providing technical assistance to Albania specifically for the implementation of chapter 27 through the "Supporting Albanian Negotiations in Environment, Chapter 27" and is focused on the creation and enhancement of the administrative capacity to successfully negotiate the Chapter[4].

Regarding the focus of the paper, Albania's energy sector differs from that of other countries in the region in that it is almost entirely based on hydroelectric electricity. Albania depends on the Drini River Basin for more than 90% of its domestic hydroelectric production[5]. This is a positive factor because Albania does not have the same problem as other countries in the region regarding dependency on coal. Yet, the country doesn't have diversified sources of energy production and depends on climate change that can decrease the river's flow and impact substantially energy supplies ane energy sector. In 2007 because of low precipitations there were significant energy shortages.

As a result of the use of hydropower, the country's emissions of carbon dioxide are lower compared to other countries in the Balkans, but the country's energy production depends on natural factors such as rainfall and on energy imports during summer or dry winters. In this context, Albania needs to enhance the production of energy from other clean energy sources like the sun and wind and especially to implement the legal framework. Some obstacles to Albania's green transition include the country's financial incapacity to enhance the use of clean energy sources in the private sector, as well as the lack of energy efficiency in buildings due to legal, social, and economic issues. Indeed, the use of solar energy in the public and private buildings in Albania will bring an economic advantage and impact the economic development of the country[6].

Over the years, the EU Commission has evidenced the unsatisfactory progress related to climate change. From 2021 to 2024, the Commission has indicated a moderated level of preparation and some progress in the energy sector and has marked the attempt to switch from exclusive use of hydropower to photovoltaic and wind renewable energy sources[7]. The mentioned progress reports of the last four years have highlighted the reliance on hydropower, the exposure to climate change that these circumstances create and the reliability of the import of energy during climate change. Climate challenges were evident last summer due to wildfires that destroyed thousands of acres of forests, while the lack of rain affected the water levels. Therefore, the utilization of alternative energy sources not only contributes to addressing climate change and achieving the objectives of the Green Agenda, but also ensures a reliance on energy production and a reduction in energy imports. Albania has tried to respond to this problem, trying to enhance the photovoltaic and renewable energy from wind but also to create other sources of energy. The 2024 Progress Report recognized the establishment and operation of the Photovoltaic Park in Karavasta, as well as the nation's efforts to diversify its energy

[1] https://integrimi-ne-be.punetejashtme.gov.al/en/negociatat/rreth-negociatave/ (11.11.2024)

[2] Artenida Duraku, Irida Agolli, *EU Integration of Chapter 27 Environment and Climate change in Albania,* "Academic Journal of Business, Administration, Law and Legal Sciences", Vol. 9, No. 3, 2023, pp. 54-61

[3]https://neighbourhood-enlargement.ec.europa.eu/document/download/75bf7bef-0ecc-40ba-893a-4d45d4ea6ddb_en?filename=factsheet_wb_green_agenda_en.pdf (12.11.2024)

[4] https://sane27.com/about-us/ (12.11.2024)

[5] Westminster Foundation for Democracy, *Monitoring of The Strategy for Climate Change and Action Plan, 2020-2030,* https://www.agora-parl.org/ (11.10.2024)

[6] Mariola Kapidani, Eni Numani, *Investing in Green Energy: Profitability Analysis of Solar Energy for Household Consumption in Albania*, "WSEAS Transaction on Business and Economics", Vol. 1, 2024, p. 345

[7] European Commission, *Progress Report Albania 2021, 2022, 2023, 2024,* https://neighbourhood-enlargement.ec.europa.eu/albania-report-2021_en (11.10.2024)

production sources[1]. Also to ulteriorly diverge the fonts of energy production an auction on wind farms was launched in 2021 but is not sufficient to guarantee the independence of energy production from hydropower[2]. The most ambitious initiative to diversify the energy font production was the participation and implementation of the Trans-Adriatic Pipeline project that is a strategic opportunity for Albania to adopt cleaner solutions for the environment[3]. However, the Pipeline remains non-operational in the country, resulting in the unavailability of gas as a source of energy production in Albania. This is due to the absence of a gas network, which necessitates significant investments in infrastructure and distribution systems within both urban and rural areas[4]. Also, the size of the market is another factor that determines the absence of the gas system. Albania has a relatively small population and lower industrial demand for gas compared to other European countries.

The progress reports also highlight the absence of secondary legislation pertaining to the Energy Performance of Building EU directive. On a positive note, the Commission appreciated the adoption of the National Energy and Climate Plan (2020-2030).

The last progress report highlights a serious concern regarding the limited alignment with the EU acquis, the country's capacity to incorporate climate change into sectorial strategies and plans, and the lack of expertise in this area[5]. The Strategy for Climate Change evidence the necessity to enhance the institutional capacities, which are fundamental for the implementation of the objectives on climate change. Increasing capacity building is one of the top priorities in response to climate change. Building institutional capacities is crucial when addressing climate change, particularly by enhancing the structure of institutions and agencies with sufficient climate-specific capacity. Climate change actions, as a relatively new approach, are not supported by adequate local, institutional, and human capacity, as evidenced by the recent progress report and monitoring reports in the country. Also, the country needs to better use the natural resources of renewable energy, especially the photovoltaic energy to assure independence from the hydropower and to diminish the import of energy during summer, considering that Albania has all the possibility to use the solar energy due to its geographic position[6]. Also, the use of solar energy offers interesting possibilities, the low cost of PV systems if incentivized in the proper way by the government but also by the local institutions is a viable option that can help reducing green gas emissions[7].

Currently, many public institutions in Albania lack the specialized knowledge, infrastructure, and resources required to develop and execute climate strategies. This gap in capacity makes it difficult to monitor emissions effectively, enforce environmental regulations, and integrate climate considerations into broader policy areas. Additionally, there is often insufficient inter-agency coordination, which hinders a unified approach to tackling climate issues across sectors. Albania's climate strategies have identified building these capacities as a national priority, emphasizing the need for training, resource allocation, and international cooperation to strengthen institutional responses to climate change[8]. This lack of capacity can risk the development and implementation of climate strategies and policies.

Indeed, the government's limited budget and staff's lack of expertise have significantly impacted the capacity of public administration. A serious corruption case involving the Tirana incinerator project surfaced in 2023, prompting the Specialized Anti-Corruption Structure to continue its investigation and several municipal directors and a former minister were arrested[9]. This fact didn't impact directly the alignment and the implementation of the EU acquis on the protection of the environment but gave space to a huge debate in the country on how the financial and human resources are being managed by the government to confront climate

[1] European Commission, *Progress Report Albania 2024*, https://neighbourhood-enlargement.ec.europa.eu/ (11.10.2024)
[2] European Commission, *Progress Report Albania 2023*, https://neighbourhood-enlargement.ec.europa.eu/ (11.10.2024)
[3] Institute for Democracy and Mediation, *Albania and the Geopolitics of the Trans-Adriatic Pipeline: Regional and Domestic Dimensions*, 2018 https://idmalbania.org/sq/news-cpt/4925/
[4] *Idem*
[5] *Idem*
[6] Aurela Qamili, Silva Kapia, *Evaluation and integration of photovoltaic (PV) systems in Albanian energy landscape, "*Solar Compass", Vol. 10, 2024, p. 3
[7] Luiza Lluri, Blerta Germenji, Eli Vyshka, Adnand Mysketa, *The Use of Photovoltaic Technology in Albania: A Good Opportunity to face the Energy Crisis*, "Interdisciplinary Journal of Research and Development", Vol. 10, No. 2, 2023, p. 25
[8] World Bank, *Albania – Climate change knowledge portal*, https://climateknowledgeportal.worldbank.org/ (11.10.2024)
[9] European Commission, *Progress Report Albania 2024*, https://neighbourhood-enlargement.ec.europa.eu/ (11.10.2024)

change. Another important focus point is the lack of inter-institutional coordination. There is a need for improved coordination among various governmental institutions involved in climate action. The current inter-institutional framework is not strong enough to facilitate effective collaboration leading to fragmenting efforts in implementing climate policies[1].

Another component of the Chapter 27 and of the Sofia Declaration is the involvement of the citizens and the information of the public on the objectives, plans, and activities that the government undertakes to ensure the green transformation and the fulfillment of the Green Agenda objectives[2]. Additionally, raising awareness about climate change issues is crucial to encourage citizens to actively participate, engage, and contribute to environmental protection, as well as to provide appropriate responses to these issues. Citizens have a crucial part in decreasing emissions through alternative energy sources, house insulation, energy management, and efficiency enhancements. This has led to only a small portion of the population taking individual actions to protect the environment and impact climate change. According to the Balkan Barometer, only 25% walk to work, 23% use public transportation, and 21% use energy efficient household appliances[3]. Additionally, the percentage of people who install solar panels is even smaller according to the same source only 8% use an electric car and 11% install solar panels for household consumption. Despite the importance of citizens' involvement in responding to climate change and the increase in their awareness, Albania still lacks a clear strategy on this issue.

The global climate crisis, particularly the recent meteorological disasters such as the floods in Valencia and Barcelona, has brought the impact of climate changes to the forefront of public discourse, yet the debate is still limited. Although the actions are being recognized as necessary by experts and the public, the debate on the climate challenges remains a principal domain of scientific circles and experts. Unfortunately, the severity of the climate changes hasn't yet received enough attention in governance, media, and education, impeding general awareness and understanding[4]. In 2023, the European Delegation in Albania, aiming to increase attention on climate change and its consequences, launched a new campaign addressing Albanian citizens, policymakers, civil society, businesses, and other stakeholders around environmental issues affecting the country[5]. Albania does not earmark financial resources for environmental protection. There is no established national environmental fund or state budget line for environment-related purposes. Furthermore, there are no established conditions for expanding public and private environmental costs. In this context, EU initiatives play a crucial role in enhancing public knowledge.

Also, the EU financial support is vital for the increase of renewable energy sources. In 2023, the EU allocated 72 million EUR through the Energy Support Package under Ipa Annual Action plan aimed at new investmens in energy sources and to mitigate the impact of the energy crisis[6]. The EU actions aim to implement the Albania's National Energy and Climate Plan's to fulfill the ambitious goal of 54.4% renewable energy into the final energy consumption by 2030 and integration aspirations[7].

We can safely assume that the EU role on the climate change initiatives in Albania and on the fulfillment of the Sofia Declaration is indispensable not only for the financial support but also for the increase of expertise and capacity in the public administration and for the increase of awareness of the public. Also, the government

---

[1] Jelena Šogorov-Vučković, Dusan Piksiades, Ivan Trifunović, *Governmental investment in the environmental economy in the Western Balkan*, "The European Journal of Applied Economics", Vol. 19, No. 1, 2022, pp. 121-136

[2] Regional Cooperation Council, *For the implementation of the Sofia Declaration on the Green Agenda for the Western Balkans 2021-2030, https://www.rcc.int/docs/596/action-plan-for-the-implementation-of-the-sofia-declaration-on-the-green-agenda-for-the-western-balkans-2021-2030* (11.11.2024)

[3] Regional Cooperation Council, *Balkan Barometer 2024*, https://www.rcc.int/balkanbarometer/results/2/public (13.11.2024)

[4] The Resource Environmental Center Albania, *Annual Report 2023*, 2024, https://ww2.recshqiperi.org/2024/11/04/annual-report-2023/ (14.11.2024)

[5] https://webalkans.eu/en/news/eu-in-albania-launches-new-awareness-campaign-on-eus-support-to-tackle-the-countrys-environmental-challenges/ (14.11.2024)

[6] https://www.eeas.europa.eu/delegations/albania/eu-transfers-eur-72-million-albania-part-energy-support-package_en?s=214 (14.11.2024)

[7] Chiara Mihalcatinova, *Is Albania a New Regional Champion in the Energy Transition?* https://www.strategicanalysis.sk/is-albania-a-new-regional-champion-in-the-energy-transition/ (14.11.2024)

should invest in grid capacity needs to enhance other infrastructure upgrade and appoint into private investments particularly into solar and wind energy[1].

Conclusions

The integration process has significantly impacted Albania, especially after the candidate status was granted in 2014. It has impacted structural reforms, the economic sector, environmental protection, and climate change. The region is struggling to cope with the consequences of natural phenomena like the flood in Bosnia Hercegovina this year or the fires in Albania the previous summer seasons. In this context, the green transition has become a priority and constitutes one of the principal integration conditions. To fulfil the membership conditions, the region became part of the Green Agenda for the Western Balkans, aiming to meet the ambitious goal of a region carbon-free until 2050. This process combats climate change by phasing out coal and converting it into renewable electricity production energy. Also, the process can boost economic growth, transform the energy sector, and attract foreign investors.

However, despite the opportunities, the green transition is affected by a series of challenges in the region that involve national and regional factors like the financial capacity and the countries' dependence on a single source of energy production. Indeed, the region depends mostly on coal, except Albania, which relies on hydropower. The use of coal increases air pollution in countries like Serbia or Bosnia Herzegovina; in Albania, the reliance on hydropower doesn't impact air pollution but leaves the country vulnerable to natural phenomena like rain and the import of energy to fulfil energy needs. So, it is of utmost relevance to the phasing out of coal and transition to renewable energy sources like wind and solar. Also, the countries need to enhance regional cooperation and collaborate with the Regional Cooperation Council to impact the green transition.

Albania has taken essential actions regarding implementing Cluster 4 – Green Agenda and Sustainable Activity - of the negotiation's accessions framework and progressing toward adopting the legal framework. Albania has adopted the National Energy Strategy (2018-2030), National Climate Change Strategy (2019), Law on Climate Change, and National Action Plan for renewable energy resources in Albania (2019-2021). It amends the National Climate and Energy Strategy to align with EU priorities. The problem that affects the country is the lack of the implementation of the legal framework due to financial factors and lack of human resources. Albania must enhance its administrative capacity by adopting a legal framework and strengthening institutional collaboration. The Commission Progress Reports define Albania as moderately prepared for climate change and some progress on the energy sector's transformation.

However, in the last year, the panorama has begun to change due to significant efforts to increase renewable energy sources that are still insufficient to cover the country's need for electricity but are a good starting point. Due to its geographical position with sunny days and mild winds, Albania has considerable potential for developing solar and wind energy. Albania has also invested in photovoltaic parks and increased the financial support to the private sector to use more solar panels. Another opportunity is the discovery of the largest hydrogen gas flow this year in Bulqize. The EU's financial support is significant in enhancing and sustaining new initiatives.

Another essential factor influencing the sector is the lack of public awareness of climate change and its consequences. Despite the topic's sensibility, the government lacks a clear strategy to involve the public in the discussion, so energy and climate problems remain a domain of academic and political circles. Raising public awareness of the importance of actions and reactions to reduce climate impact through daily life is indispensable. Also, there are no sufficient initiatives and financial capacity to support using renewable energy sources like the solar panel for domestic purposes. The EU and other donors like the Swedish government are developing continuous campaigns to enhance public awareness and engage citizens on environmental protection. In this context, Albania has taken important steps and has progressed to the green transition overall, but it needs to increase the implementation of the legal framework and elaborate clear strategies to raise public awareness.

[1] Dimitar Bechev, *The Green Transition and the Western Balkans*, "Carnegi Europe", 2024 https://carnegieendowment.org/research/2023/10/the-green-transition-and-the-western-balkans?lang=en&center=europe (13.11.2024)

Bibliography

Books

1. Radovic, Markovic, M.; Jovancevic, D.; Nikitovic, Z., *Toward green economy: opportunities and obstacles for Western Balkan countries*, Xlibris Publishing, Bloomington, 2016

Studies and Articles

1. Duraku, Artenida; Agolli, Irida, *EU Integration of Chapter 27 Environment and Climate change in Albania*, "Academic Journal of Business, Administration, Law and Legal Sciences", Vol. 9, No. 3, 2023
2. Ignjatović, Jelena; Filipović, Sanja; Radovanović, Mirjana, *Challenges of the Green Transition for the Recovery of the Western Balkans*, "Energy Sustainability and Society", Vol. 14, No. 2, 2024 doi: 10.1186/s13705-023-00421-4
3. Gibbs, David; O' Neill, Kirstie, *Future Green Economies and Regional Development: a research Agenda*, "Regional Studies", Vol. 15, No. 1, 2017
4. Kapidani, Mariola; Numani, Eni, *Investing in Green Energy: Profitability Analysis of Solar Energy for Household Consumption in Albania*, "WSEASTransaction on Business and Economics", Vol. 1, 2024
5. Dunjic, Stefan; Pezzutto, Simon; Zubaryeva, Alyona, *Renewable Energy development trends in the Western Balkans*, "Renewable and Sustainable Energy Reviews", Vol. 65, 2016 https://www.sciencedirect.com/science/article/abs/pii/S1364032116301630?via%3Dihub
6. Filipovic, Sanja; Noam, Lior; Radonavic, Mirjana, *The Green Deel – just transition and sustainable development goals Nexus*, "Renewable and Sustainable Energy Reviews", Vol. 168, 2022 https://www.sciencedirect.com/science/article/abs/pii/S136403212200644X?via%3Dihub
7. Lluri, Luiza; Germenji, Blerta; Vyshka, Eli; Mysketa, Adnand, *The use of Photovoltaic Technology in Albania: A Good Opportunity to Face the Energy Crisis*, "Interdisciplinary Journal of Research and Development, Vol. 10, No. 2, 2023
8. Qamili, Aurela; Kapia, Silvia, *Evaluation and integration of photovoltaic (PV) systems in Albanian energy landscape*, "Solar Compass", Vol. 10, 2024 https://doi.org/10.1016/j.solcom.2024.100070
9. Durcevic Miljana*, European Union's practice turn in "Green" Policies in the Western Balkans Accession Negotiations*, "Science International Journal", Vol. 3, No. 4, 2024 https://doi.org/10.35120/sciencej0304181d
10. Šogorov-Vučković, Jelena; Piksiades, Dusan; Trifunović, Ivan, *Governmental investment in the environmental economy in the Western Balkan*, "The European Journal of Applied Economics", Vol. 19, No. 1, 2022

Documents

1. Aspen Institute, *Green Agenda for the Western Balkans*, 2023, https://www.aspeninstitute.de/wp-content/uploads/Green-Agenda-for-the-Western-Balkans_2023.pdf
2. Carnegie Europe, *The Green Transition and the Western Balkans*, 2023, https://carnegieendowment.org/research/2023/10/the-green-transition-and-the-western-balkans?lang=en
3. European Commission, *Progress Report Albania*, 2021, https://neighbourhood-enlargement.ec.europa.eu/albania-report-2021_en
4. European Commission, *Progress Report Albania*, 2022, https://neighbourhood-enlargement.ec.europa.eu/albania-report-2022_en
5. European Commission, *Progress Report Albania*, 2023, https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_690%20Albania%20report.pdf
6. European Commission, *Progress Report Albania*, 2024, https://neighbourhood-enlargement.ec.europa.eu/
7. Institute for Democracy and Mediation, *Albania and the Geopolitics of the Trans-Adriatic Pipeline: Regional and Domestic Dimensions*, 2018
8. IGN Agora Energiewende, *Powering the future of the Western Balkans with Renewables*, 2021 https://www.agora-energiewende.org/fileadmin/user_upload/2021-01_EU_Balkan_Green_Deal.pdf
9. Regional Cooperation Council, *Green Agenda*, 2020, https://www.rcc.int/greenagenda
10. Regional Cooperation Council, *Balkan Public Barometer*, 2024 *https://www.rcc.int/balkanbarometer/home*

11. REC Albania, *Annual Report*, 2023, https://ww2.recshqiperi.org/2024/11/04/annual-report-2023/
12. OECD Development Pathways, *Multi-dimensional Review of the Western Balkans: From Analysis to Action*, 2022, https://www.oecd.org/en/publications/multi-dimensional-review-of-the-western-balkans_8824c5db-en.html
13. Westminster Foundation for Democracy, *Monitoring of The Strategy for Climate Change and Action Plan, 2020-2030*, 2024, https://www.agora-parl.org/
14. Zvezdanović, Lobanova, Jelena, *The Green Transition and Energy Security in the Western Balkans Countries*, 2024 https://doi.fil.bg.ac.rs/pdf/eb_book/2024/iipe_gsirescu/iipe_gsirescu-2024-ch24.pdf

Websites

1. https://integrimi-ne-be.punetejashtme.gov.al/
2. https://neighbourhood-enlargement.ec.europa.eu/
3. https://sane27.com/about-us/
4. https://webalkans.eu/en/news/
5. https://www.rcc.int/
6. https://www.strategicanalysis.sk/
7. https://www.wbif.eu/

Dumitru BUDACU
Alexandru Ioan Cuza University of Iași, Romania

THE IMPACT OF THE ARTIFICIAL INTELLIGENCE ON HYBRID CONFLICTS IN THE 21ST CENTURY

Abstract:	*Hybrid conflict, from an artificial intelligence perspective, refers to complex and multifaceted conflict in which different methods of warfare are used in a coordinated manner to achieve strategic objectives. Artificial intelligence can play a significant role in both executing and defending against 21st century conflicts. Hybrid conflicts are characterized by the blending of conventional and unconventional tactics, often involving a combination of military force, cyber operations, economic coercion and information warfare. Some notable examples where elements of hybrid conflict have been observed are Russia – Ukraine Conflict (2014 – present), Syrian Civil War (2011 – present), Crimea Annexation (2014), Iranian Proxy wars and Cyber Operations, China's Strategy in the South China Sea, Baltic states and Russian Influence Operations. The role of artificial intelligence in countering Hybrid conflict is to detect and analyze threats, shape automated response systems, support strategic decisions, and build resilience.* *The impact of artificial intelligence on hybrid conflict in the 21st century is profound and multifaceted. While offering significant advantages in intelligence, cyber operations and decision-making, it also introduces new risks and ethical dilemmas. As artificial intelligence continues to evolve, its role in hybrid conflicts is likely to expand, becoming a key factor in future military and geopolitical strategies. To meet these challenges, it is essential that nations develop robust frameworks for responsible use of artificial intelligence in warfare, ensuring that its benefits are exploited while minimizing risks. It is certain that the ability of AI to quickly and accurately process and analyze large amounts of information, which can be exploited to either execute or counter these multifaced strategies, will be a major challenge for all of us in the years ahead.*
Keywords:	**Artificial intelligence; conflict; ethics; hybrid conflict; operations; tactics;**
Contact details of the authors:	E-mail: budacu_dumitru@yahoo.com
Institutional affiliation of the authors:	**Alexandru Ioan Cuza University of Iași, Romania**
Institutions address:	Bulevardul Carol I, Nr.11, 700506, Iaşi, România, 0040/0232 20 1000, www.uaic.ro

Terminology clarifications

For our study we have used two concepts, namely artificial intelligence and conflict. In the following, we will briefly specify these two concepts.

Artificial intelligence. Emergence and evolution

Intelligence is the capacity of a being to learn, understand and use knowledge and skills and abilities to solve problems, adapt behavior to new situations, make decisions and create innovative solutions. This involves complex brain processes such as perception, reasoning, memory, creativity and the ability to make logical connections. According to different psychological theories, there are several types of intelligence: *logical-mathematical intelligence* (the ability to think logically, solve problems and work with mathematical concepts), *linguistic intelligence* (the ability to use language to communicate effectively, to write and to understand the subtleties of language), *spatial intelligence* (the ability to visualize objects and spaces and

understand the relationships between them), *interpersonal intelligence* (the ability to understand and interact well with other people), *intrapersonal intelligence* (the ability to understand oneself, to recognize one's own emotions and to manage them), *naturalistic intelligence* (the ability to understand and interact effectively with the environment), and *kinesthetic intelligence* (the ability to use one's own body to express ideas and perform physical activities).

Moreover, in recent years the concept of artificial intelligence has become increasingly relevant. Artificial intelligence refers to the ability of computers and machines to mimic some of the functions of human intelligence, such as pattern recognition, natural language processing, decision making and even learning. The term artificial intelligence was first used in 1956 by the American computer scientist John McCarthy, who is considered one of the fathers of the field. McCarthy introduced the term at a conference held at Dartmouth College in Hanover, New Hampshire, to investigate the possibilities of creating machines capable of simulating human cognitive processes. While initially the term artificial intelligence was used to designate any effort to make machines "intelligent", i.e. capable of mimicking or simulating human cognitive functions, today artificial intelligence has become a general term for a vast field that includes *machine learning* (algorithms that learn from data and improve performance over time), *deep learning* (complex neural network models, used for tasks such as facial recognition or machine translation), *natural language processing* (understanding and generating human text and speech) and *general artificial intelligence* (a theoretical concept of an artificial intelligence capable of a wide range of human-like cognitive tasks).

The term artificial intelligence, originally used to describe attempts to create machines that can 'think' like humans, has since become synonymous with a broad field of science that is increasingly influencing many aspects of modern life, and certainly in the future our lives will certainly be influenced and changed by artificial intelligence. To this distinctive capacity our species owes its dominant position. If machine brains surpass human brains in general intelligence, then this new superintelligence could become extremely powerful, possibly beyond our control[1].

Deep learning is a form of machine learning that allows computers to learn from experience and understand the world in terms of a hierarchy of concepts. Because the computer accumulates knowledge from experience, there is no need for a human computer operator to formally specify all the knowledge the computer needs. Concept hierarchies allow the computer to learn complicated concepts by building them from simpler concepts; a graph of these hierarchies would have many layers of depth. This book covers a wide range of topics in deep learning[2]. Reinforcement learning, one of the most active areas of research in artificial intelligence, is a computational approach to learning in which an agent attempts to maximize the total amount of reward it receives when interacting with a complex and uncertain environment[3]. Deep learning has stimulated the whole field of machine learning[4]. Inevitably we can turn to a few questions when it comes to artificial intelligence, namely How smart are the best artificial intelligence programs really? How do they work? What can they do and when do they fail? How human-like do we expect them to become, and how quickly do we need to worry that they'll outperform us? Along the way, she introduces the dominant models of modern artificial intelligence and machine learning, describing cutting-edge artificial intelligence programs, their human inventors, and the historical lines of thought underlying recent achievements[5].

To conclude by saying that artificial intelligence powers Google's search engine, allows Facebook to target advertising, and allows Alexa and Siri to do their jobs. AI also underpins self-driving cars, predictive policing and autonomous weapons that can kill without human intervention. These and other applications of AI raise complex ethical issues that are the subject of ongoing debate[6].

The concept of conflict. Evolution and diversity

The general term conflict can be understood as a situation in which two or more parties (individuals, groups, organizations or even countries) have interests, needs, values or goals that are opposed or incompatible and lead to tensions, disagreements or confrontations. Conflicts can arise in different contexts (in personal

[1] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2016, p. 57
[2] Ian Goodfellow, Yoshua Bengio Courville, *Deep Learning*, The MIT Press, 2016, p. 33
[3] Andrew C. Barto, Richard S. Sutton, *Reinforcement Learning: An Introduction*, Bradford Books, 2018, p. 19
[4] Aurélien Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, And TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O'Reilly Media, 2019, p. 47
[5] Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Human*. Farrar, Straus and Giroux, 2019, p. 98
[6] Mark Coeckelbergh, *AI Ethics*, The MIT Press, 2020, p. 44

relationships, at work, in society or internationally). Conflicts are of different types *interpersonal conflict* (between individuals because of personality differences, opinions or disagreements), *intra-personal conflict* (occurs within a person, when they are faced with difficult choices, internal contradictions or conflicts between their own values and desires), *group conflict* (occurs between groups/teams with different goals, values or interests), *organizational conflict* (occurs within an organization and may be related to differences in business priorities, management styles or available resources), and *international conflict* (occurs between nations/large groups of people and may include political, economic or military conflicts).

The causes of conflict can be: *different interests* (when two parties want opposing things), *differences in values* (when personal, cultural or religious values clash), *limited resources* (competition for scarce resources can lead to conflict), *poor communication* (lack of clear communication or misunderstandings can lead to tensions), *different perceptions* (how parties interpret a situation can create conflict, even if intentions are good). Resolving a conflict usually involves identifying the causes and finding a compromise. Settlement methods are diverse and can include *negotiation* (direct discussions to reach a solution that satisfies both parties), *mediation* (a neutral third party helps the parties find a solution), *arbitration* (an external person or conflict makes a binding decision for both parties), *dialog* and *active listening* (understanding each party's perspectives and needs to reach a common solution). Conflicts are a natural part of human interaction, and the way they are managed can either lead to peaceful resolution or escalation.

A *military conflict* is a violent confrontation between two or more parties, usually states or organized armed groups, in which armed forces are used to gain control over resources, territory or to impose their political will. Military conflicts range from small, small-scale confrontations to large-scale wars involving land, air and naval forces. The most common types of military conflicts are: *war* (extreme form of military conflict, with large-scale fighting between nations or coalitions of nations), *civil war* (conflict between groups or factions within the same country, usually over political power or independence), *asymmetric conflict* (occurs when a state or conventional army fights against a smaller force, such as insurgent or terrorist groups, using guerrilla tactics), *military intervention* (involves sending troops into another country to support or overthrow a government without a declaration of war), *limited military conflict* (a conflict between two or more countries that avoids full escalation of war, usually restricted to certain borders or regions).

What is most painful after a military conflict are its consequences. The consequences of a military conflict are: *loss of life* (a large number of military personnel are killed or wounded, as well as inevitably the collateral victims who are civilians, namely women, children and the elderly), *destruction of infrastructure* (military confrontations leave behind destroyed cities, roads and other structures), *humanitarian crises* (conflicts lead to refugees famine, lack of clean drinking water and other hardships for affected populations), *economic impact* (resources are squandered, trade is affected, and reconstruction costs are huge), *political* and *social instability* (wars destabilize affected regions, often leaving room for post-conflict chaos and violence). Inevitably any conflict and military conflicts can be resolved. The resolution of military conflicts involves *peace negotiations* (the two sides meet to discuss the terms of cessation of hostilities), *armistice agreements* (the two sides agree to temporarily or permanently cease hostilities), *international mediation* (international organizations such as the UN intervene to facilitate peace talks), *peacekeeping intervention* (peacekeeping troops are sent in to protect civilians and prevent the conflict from restarting). *Military conflicts* are among the most serious forms of conflict, with complex and long-lasting effects on societies and economies worldwide.

A *hybrid conflict* is a form of modern conflict that combines conventional (classical military) tactics with unconventional tactics (such as disinformation, cyber-attacks and subversive actions) to destabilize or influence an adversary without initiating an open military confrontation. In this type of conflict, the aggressor combines a variety of methods - *military*, *economic*, *political* and *informational* - to weaken a state or organization without attracting the international attention and retaliation that would be involved in a traditional war.

When referring to *the military methods* used in hybrid warfare, it should be kept in mind that hybrid warfare is a complex strategy in which conventional and unconventional tactics are used to destabilize, intimidate and undermine a target without directly engaging conventional forces. In this type of conflict, *military methods* are interwoven with *non-military actions* (such as information manipulation, cyber-attacks and political subversion) to gain strategic advantage. The main military methods used in hybrid warfare are: the use of special troops and clandestine forces, psychological operations and propaganda, propaganda and media manipulation, cyber-attacks, cyber warfare, information warfare, unconventional and asymmetric

weapon systems, instigation of protest movements and riots, support of local actors or military groups, exploitation of ethnic and religious conflicts, economic mobilization and financial pressures, and the creation of "grey zones" and strategic ambiguity. The military methods of hybrid warfare are complemented by a wide range of unconventional and asymmetric techniques, which allow the attacking state to weaken the target without a conventional invasion. These tactics undermine the stability and responsiveness of the targeted country and create strategic ambiguity that makes international responses difficult.

The economic methods used in hybrid warfare are tactics of influence and economic pressure designed to weaken the target state, cause financial instability and reduce its ability to respond to other forms of aggression. These economic methods are often subtle and difficult to attribute to an attacking state, helping to maintain a "gray zone" in which responsibility is difficult to determine. Some of the main economic methods most often used in hybrid warfare are: economic sanctions and embargoes, currency and financial market manipulation, cyber-attacks on the financial system, corruption and subsidization of local economic groups, control over energy resources and supply, strategic investigations and the purchase of critical assets, economic sabotage and price manipulation, support for corruption and the underground economy, undermining confidence in financial institutions, creating economic dependence through credit and loans, and cornering the economic media market. These economic methods of hybrid warfare are part of a broader strategy of destabilization and influence, in which the attacking state attempts to weaken the economy without resorting to direct military confrontation. Tactics such as economic sanctions, manipulation of markets, support for the underground economy and strategic investment allow the aggressor to exert pressure on governments and influence the target country's economic and political decisions. In this way, economic warfare becomes a central component of hybrid warfare, helping to gain strategic advantage without escalating the conflict militarily.

The political methods of hybrid warfare are tactics designed to weaken the political stability, social cohesion and credibility of target governments without the use of direct military force. These tactics involve manipulating information, influencing political decisions and undermining public confidence in democratic institutions. These are just some of the political methods used in hybrid warfare: Undermining trust in state institutions, interfering in electoral processes, widespread propaganda and disinformation, supporting protest movements and the opposition, influencing government policies through agents of influence, creating and sustaining ethnic and religious conflicts, launching campaigns to delegitimize political leaders, promoting separatism and regional autonomy, influencing through cultural and ideological tools, using international organizations and diplomacy for pressure, co-opting and corrupting local media, undermining legislation and the rule of law. The political methods of hybrid warfare are designed to weaken the target state through subtle and indirect actions. Tactics such as disinformation, election meddling, support for separatist movements and instigation of ethnic conflicts contribute to political destabilization and division of society. These actions have a major impact on public confidence in the government and state institutions, making them vulnerable to further aggression and reducing national resilience.

The information methods in hybrid warfare are tactics by which the aggressor state manipulates information to influence public opinion, create confusion, undermine trust in government and weaken social cohesion. These methods use a variety of channels, from the media and social networks to cyber-attacks, and are essential in hybrid warfare because they allow the attacking state to exert indirect control over the perceptions and actions of the target state. The main information methods used in hybrid warfare are: disinformation (fake news), propaganda, psychological warfare, creation and distribution of conspiracy theories, manipulation of social networks, cyber-attacks on media and communication institutions, co-opting and influencing local media, intervention in external information flows (geo-blocking and geolocation), spying and data collection for manipulation, distortion or taking real information out of context, creation of "alternative sources" and fake news sites, flooding and manipulation of images and video content. Information methods in hybrid warfare are essential to destabilize the target state without resorting to direct violence. Through tactics of disinformation, propaganda and cyber-attacks, the attacking state can influence public perceptions, weakening trust in government and fragmenting social cohesion. These methods are difficult to counter, as they work subtly and blend into the daily lives of the target population, thus contributing to the aggressor's goals of an undeclared conflict strategy. Hybrid warfare is increasingly relevant today, with several high-profile examples demonstrating its use by state and non-state actors. Here are some of the most notable examples:

Russia's invasion of Ukraine (2022 - present)

Russia's large-scale invasion of Ukraine in 2023 exemplifies hybrid warfare, combining traditional military force with irregular tactics such as the use of mercenaries from groups like the Wagner Group. Russia has launched numerous cyberattacks against Ukraine, targeting critical infrastructure, government networks, and communications systems to disrupt Ukraine's defenses and governance. Disinformation campaigns have been used to manipulate domestic and international perceptions of the conflict, including spreading false reports about the reasons for the invasion, the nature of the conflict and the legitimacy of the Ukrainian leadership. Russia has used electricity supplies as leverage against European countries supporting Ukraine, reducing or cutting off gas supplies to create economic and political instability. The Russian invasion of Ukraine has been a significant and ongoing event, generating a substantial body of literature that examines the conflict from various angles, including military strategy, geopolitical implications and humanitarian impact.

When it comes to the conflict between Russia and Ukraine, it is certain that Russia's rapid rise to power over the past few years coupled with a stunning lack of international diplomacy on the part of its president, combined with the rapidly changing geopolitics of Europe, has led to the West being on a possible path to nuclear war, as is becoming increasingly clear in the Russia versus Ukraine conflict[1]. Today, Russia, the successor to the Soviet Union, has put Ukraine's independence back in its sights[2]. Ukraine is currently embroiled in a tense struggle with Russia to preserve its territorial integrity and political independence, but today's conflict is just the latest in a long history of struggles over Ukraine's territory and its existence as a sovereign nation[3]. New game-changing technologies, disappearing rules of the game, and distorted perceptions on both sides combine to lock Washington and Moscow into an escalating spiral they don't recognize. All the pieces are in place for a World War I-type tragedy that could be triggered by a small and unpredictable event. The Russia Trap shows that anticipating this danger is the most important step in preventing it[4]. One thing is certain and that is that neither side has been able to bring this conflict to a definitive conclusion[5]. The seeds of Russia's war against Ukraine and the West were sown more than a decade before. Ukraine in all its splendor: vast, defiant, resilient and full of wonder[6].

China's activities in the South China Sea

China uses a combination of its navy, coast guard and maritime police to assert its territorial claims in the South China Sea, including building artificial islands and militarizing them, as well as deploying fishing fleets to exercise control over disputed areas. China engages in “legal warfare” by using ambiguous interpretations of international law, particularly the United Nations Convention on the Law of the Sea (UNCLOS) to justify its actions. China also uses economic coercion such as trade restrictions against countries that challenge its claims. China uses state media and social media to promote its “narrative” on the South China Sea, attempting to legitimize its actions and discredit the opposing claims of other nations such as Vietnam and the Philippines.

China's rise on the world's oceans is attracting particular attention and could ultimately reshape the global balance of power during the 21st century[7]. The topic of whether and how to integrate a stronger China into a global maritime security partnership has not been adequately explored. But for practitioners to structure cooperation effectively, they warn, Washington and Beijing need to create sufficient political and institutional space. China's maritime power dates back thousands of years. China has one of the oldest naval traditions in the world. However, China has historically been a mainland state with a large land force and only a coastal navy with limited blue-water capability. The rise of modern China raises considerable regional and security issues, in addition to the economic and political competition for a rightful place in the power politics of the South Asian region, and therefore requires critical analysis. It is necessary to focus future strategies to meet

[1] Richard Shirreff, *War with Russia: An Urgent Warning from Senior Military Command*, Quercus, 2016, p. 47
[2] Anne Applebaum, *Red Famine: Stalin's War on Ukraine*, Doubleday, 2017, p. 11
[3] Serhii Plokhy, *The Gates of Europe: A History of Ukraine*, Basic Books, 2017, p. 19
[4] George Beebe, *The Russia Trap: How Our Shadow War with Russia Could Spiral into Catastrophe*, Thomas Dunne, 2019, p. 71
[5] Lawrence Freedman, *Ukraine and the Art of Strategy*, Oxford University Press, 2019, p. 88
[6] Christopher Miller, *The War Came to Us: Life and Death in Ukraine*, Bloomsbury Continuum, 2023, p. 54
[7] Andrew S. Erickson, Lyle J. Goldstein, Nan Li, *China, the United States, and 21st-Century Sea Power: Defining a maritime Security Partnership*, Naval Institute Press, 2010, p. 22

these challenges, both in the medium and long term[1]. The rise of China has upset the global balance of power. For decades, tensions have simmered in the region, but now the threat of direct superpower confrontation is becoming increasingly likely. Whoever controls these waters controls access between Europe, the Middle East, South Asia and the Pacific[2]. Over the past decade, the center of world power has quietly shifted from Europe to Asia. With oil reserves of several billion barrels, an estimated nine hundred trillion cubic meters of natural gas, and competing territorial claims dating back centuries, the South China Sea in particular is a boiling pot of potential conflict. The buildup of military forces in the area where the Western Pacific meets the unreported Indian Ocean means that this is likely to be a fulcrum for global war and peace for the foreseeable future. To understand the future of conflict in East Asia, we need to understand the goals and motivations of its leaders and people, at a time when every day's news seems to contain a new story, big or small, that is directly related to the conflicts in the South China Sea[3]. Great Powers, Great Strategies offers the analysis of a dozen experts on "global" approaches to the South China Sea dispute. By exploring the international dimensions of this regional hotspot, it is worth examining how the military, diplomatic and economic strategies of major global actors have contributed to solutions and exacerbated the potential for conflict[4].

Iran's regional influence operations

Iran supports various proxy groups in the Middle East, such as Hezbollah in Lebanon, the Houthis in Yemen and Shiite militias in Iraq and Syria. These groups conduct military operations and terrorist activities that analyze Iranian interests without Iran's direct involvement. Iran has been linked to cyber-attacks targeting critical infrastructure and government institutions in rival countries, including Saudi Arabia and Israel. Iran also uses cultural diplomacy, media and religious ties to influence political outcomes in neighboring countries. Worth analyzing is how the struggles between Shiites and Sunnis in the Middle East will affect the future of the region, offering insight into the brutal and long-running power struggles between Iran and Saudi Arabia for political and spiritual leadership of the Muslim world[5].

The United States and Iran have been engaged in an unrecognized secret war since the 1970s. This conflict has frustrated several US presidents, divided administrations and repeatedly threatened to bring the two nations to the brink of open war. From the Iranian Revolution to the secret negotiations between Iran and the United States after 9/11, from Iran's nuclear program to Qasem Soleimani's covert and lethal role, a vital new depth to our understanding of the "Iranian problem" and what the future may bring to this tense relationship represents one of the most significant challenges[6].

In recent years, significant attention has focused on the Islamic Republic of Iran's nuclear ambitions and the threat they pose to the United States and the West. Much less understood, however, has been the phenomenon of Iran's regional advance into America's own hemisphere, an intrusion that has both foreign policy and national security implications for the United States and its allies[7].

Another important challenge is to analyze how the Arab world got to this point, what is happening now, what the ramifications will be, how it will affect Israel, and what immediate actions need to be taken, including how Western leaders should respond. Consider all the major power players in the Middle East, the underlying issues, the Arab Spring, the fall of the Muslim Brotherhood, the rise of ISIS, the epic animosity between Sunni and Shia, the essence of the Syrian war, the role of the caliphate and jihad, and the impending nuclear arms race[8]. We are obligated to get to know these people - what the regime means to them and their

[1] Sandeep Dewan, *China's Maritime Ambitions and the PLA Navy*, Vij Books India, 2013, p. 17

[2] Bill Hayton, *The South China Sea: The Struggle for Power in Asia*, Yale University Press, 2014, p. 81

[3] Robert D. Kaplan, *Asia's Cauldron: The South China and the End of a Stable Pacific*, Random House Trade Papperbacks, 2015, p. 73

[4] Andreas Corr, *Great Powers, Grand Strategies: The New Game in the South China Sea*, Naval Institute Press, 2018, p. 54

[5] Vali Nasr, *The Shia Revival: How Conflicts within Islam Will Shape the Future*, W. W. Norton & Co Inc, 2007, p. 17

[6] David Crist, *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran*, Penguin Publishing Group, 2013, p. 77

[7] Ilan Berman, Joseph M. Humire, *Iran's Strategic Penetration of Latin America*, Lexington Books, 2016, p. 27

[8] Avi Melamed, *Inside the Middle East: Making Sense of the Most Dangerous and Complicated Region on Earth*, Skyhorse, 2016, p. 91

anxieties about the future of their revolutionary project, of what it means to be pro-regime in the Islamic Republic, challenging everything we think we know about Iran and revolution[1].

North Korea's cyber operations

North Korea has increasingly relied on cyberattacks as a means of hybrid warfare, targeting financial institutions, cryptocurrency exchanges and critical infrastructure around the world. I would mention among notable attacks only the Sony Pictures hack (2014) and the WannaCry ransomware attack (2017). Through cyber operations, North Korea is trying to evade international sanctions and finance its regime, so it has stolen billions of dollars through cyber heists, especially from cryptocurrency exchanges. North Korea uses cyber capabilities to spread propaganda and disinformation to influence perceptions and destabilize adversaries, both domestically and internationally. Identity Wars is a wide-ranging look at how anonymity influences politics, activism, religion and art. A firm defense of anonymity and exploration of certain tools and organizations, especially its evolution with the ubiquity of the internet is of utmost importance. Examining online identities, both fake and real, is essential reading for the age of social networks[2]. Cybersecurity always in the era of cyber conflict has played a significant role for all state actors, including North Korea[3].

Turkey's use of hybrid tactics in Syria and Libya

In Syria, Turkey supported various rebel groups against the Assad regime and Kurdish forces. In Libya, Turkey provided military and logistical support to the Government of National Accord (GNA) against the Libyan National Army (LNA). Turkey effectively used drones in these conflicts, providing air support to its close allies, carrying out strikes on targets of opposition forces. Turkey has used the media and social media to shape accounts of its involvement in these conflicts, presenting its actions as part of a broader strategy to promote regional stability and combat terrorism. Turkey's use of hybrid tactics in Syria and Libya is a complex and multifaceted topic, covering aspects of military strategy, political maneuvering, and influence operations. Turkey holds a unique position between East and West and, with the end of the Cold War, has the potential for influence. Freedom from the Russian threat allows it to examine its ties with the West, and political changes and shifts in power in the region give it the opportunity to forge new relationships with its neighbors in the Near and Middle East[4]. Of particular importance is the exploration of how Turkey's contested national identity has affected its foreign policy from the end of the Ottoman era to the present. Identity matters for foreign policy decisions, but it separates itself from etatist approaches by bringing the issue of identity into domestic politics[5]. Hybrid warfare has been an integral part of the historical landscape throughout the ages, but recently analysts have incorrectly labeled these conflicts as unique. Throughout history, great powers have faced adversaries that have used a combination of regular and irregular forces to nullify the advantage of the great power's superior conventional military force. Hybrid wars are labor-intensive and long-term affairs. Hybrid wars are also the most likely conflicts of the 21st century, as competitors use hybrid forces to deplete military capabilities in protracted campaigns of exhaustion[6].

The effects of the Arab Spring on Turkish foreign policy are worth investigating. The demands for democracy that began in Tunisia spread rapidly across the Arab Middle East and North Africa. The focus and dynamics of the Arab Spring varied according to the countries in which it took place. As a counterpoint to the status quo in the Middle East, the Arab Spring stimulated much debate, leading to the emergence of new regional actors[7]. It is also worth examining contemporary political relations between Turkey and the Middle East. In the light of the 2011 Arab uprisings, the Syrian crisis, the escalation of regional terrorism and the attempted military coup in Turkey, the dramatic fluctuations in Turkey's foreign policy towards the major Middle Eastern countries of Iran, Saudi Arabia, Egypt, Syria and Iraq are also worth analyzing, as well as the analysis of Turkey's deepening involvement in regional affairs in the Middle East, also addressing issues such

[1] Narges Bajoghli, *Iran Reframed: Anxieties of Power in the Islamic Republic*, Stanford University Press, 2019, p. 84
[2] Cole Stryker, *Hacking the Future: Privacy, Identity, and Anonymity on the Web*, Abrams Press, 2012, p. 77
[3] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2017, p. 61
[4] Barkey, Henry, J., *Reluctant Neighbor: Turkey's Role in the Middle East*, United States Institute of Peace, 1997, p. 77
[5] Hasan Kösebalaban, *Turkish Foreign Policy: Islam, Nationalism, and Globalization (Middle East Today)*, Palgrave Macmillan, 2011, p. 62
[6] Williamson Murray, Peter R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012, p. 15
[7] Ýdris Demir, *Turkey's Foreign Policy Towards the Middle East: Under the Shadow of the Arab*, Cambridge Scholars Publishing, 2016, p. 33

as terrorism, social and political movements and struggles for minority rights. While these issues have traditionally been seen as domestic matters, this book emphasizes their increasingly regional dimension and the implications for the foreign affairs of Turkey and the countries of the Middle East[1].

The understanding of contemporary Turkey also involves the historical, sociological and political-economic analysis of Turkish politics through the methodological localization of Turkish governance at the intersection of global-regional-national-local interactions of Turkish politics, exceptional in its analytical and methodological richness and explanatory power[2]. The issues relevant to Turkey today, such as consolidating democracy, addressing problems related to economic development, improving its human rights situation and its foreign policy, in a historical context, allow comparisons with other countries in the world that developed late and reflect the complexity of Turkey's political and socio-economic developments. Turkey's modernization process started in the 19th century with all its elements, including secularization and westernization[3].

Russian Georgian conflict (2008)

The 2008 Russian Georgian war is often seen as a precursor to modern hybrid conflicts, although it also involved direct military confrontations. Before and during the military conflict, Georgia's digital infrastructure was repeatedly attacked by Distributed Denial of Service (DDoS) attacks, which affected communications and disrupted the Georgian government's ability to coordinate. Russia used the media to disseminate narratives justifying military intervention in South Ossetia and Abkhazia. These regions have been supported by Russia in their efforts to secede from Georgia, and Moscow has used this conflict to expand its influence in the region. The 2008 Russo-Georgian conflict, often referred to as the Russo-Georgian War, has been the subject of much analysis, historical accounts and political commentary. In the summer of 2008, a conflict that seemed to have started in the Georgian breakaway territory of South Ossetia escalated rapidly into the most important European security crisis of the last decade. The implications of the Russo-Georgian war will be understood differently, depending on how one tells the story of what happened and one's perspective on the wider context[4].

The short-lived war between Russia and Georgia in August 2008 seemed too many to be an unexpected bolt out of the blue that disappeared as quickly as it appeared. A small war that shook the world is a fascinating look at the collapse of relations between Russia and the West, the disintegration and decline of the Western Alliance itself, and the fate of Eastern Europe in a time of economic crisis[5]. The Caucasus is often treated as a side-plot in Russia's history or a mere gateway to Asia, the five-day war in Georgia, which turned into a major international crisis in 2008, proves that it is still a combustible region whose internal dynamics and history deserve a much more complex appreciation by the world at large[6]. Georgia emerged from the fall of the Soviet empire in 1991 with the promise of rapid economic and democratic reform. But that promise remains unfulfilled. Economic collapse, secessionist provocations, civil war and failure to escape the legacy of Soviet rule, culminating in the 2008 war with Russia, characterize a two-decade struggle to establish democratic institutions and consolidate statehood. A broader critical analysis of Georgia's recent political and economic development illustrates what its "transition" has meant not only for the state but also for its citizens. An authoritative and compelling exploration of Georgia since independence is essential for those interested in the post-Soviet world[7].

Conflicts in the Baltic region (Estonia, Latvia, Lithuania)

The Baltic countries, which have significant Russian populations, are often targets of Russian disinformation campaigns and cyber-attacks. Following a dispute over the relocation of a Soviet monument, Estonia was the target of massive cyber-attacks, targeting government institutions, banks and communication networks. These attacks are considered the first major cyber-attacks against a state. Russia has used media and

[1] Hüseyin Işikal, Oğuzhan Göksel, *Turkey's Relations with the Middle East: Political Encounters after the Arab Spring*, Springer, 2018, p. 97

[2] Ziya Öniş, Fuat E. Keyman, *Turkish Politics in a Changing World: Global Dynamics and Domestic Transformations*, Istanbul Bilgi University Yayinlari, 2007, p. 27

[3] Meliha Altunisik, Ozlem Tur, *Turkey: Challenges of Continuity and Change*, Routledge, 2022, p. 99

[4] Cornell E. Svante, Frederick S. Starr, *The Guns of August 2008: Russia's War in Georgia*, Routledge, 2009, p. 66

[5] Ronald Asmus, *Little War That Shook the World: Georgia, Russia, and the Future of the West*, St. Martin′s Press, 2010, p. 18

[6] Thomas de Wall, *The Caucasus: An Introduction*, Oxford University Press, 2010, p. 39

[7] Jones F. Stephen, *Georgia: A Political History Since Independence*, I. B. Tauris, 2012, p. 88

social networks to disseminate narratives aimed at dividing Baltic societies and promoting Russian interests. The aim is often to sow mistrust between the Russian minority and the governments of these countries and to undermine solidarity within NATO and the EU. The Baltic region, which includes Estonia, Latvia and Lithuania, has had a rich and complex history, marked by conflicts, occupations and struggles for independence.

The world's attention has focused on the newly independent Baltic states of Latvia, Estonia and Lithuania, which are struggling to become politically and economically viable. The history and culture of the Baltic states, from their ancient origins to their contemporary status, their religious and racial differences, their relations with Russia and the West and their prospects for the future, their new constitutions and the 1992 elections, the current forces of law and order, the demolition of the Soviet economies and the possibilities of democracy and Europeanization or ethnic conflict and nationalist dictatorship, are of particular importance to our study[1]. Since the end of the Cold War there has been increased interest in the Baltic countries. Estonia, Latvia and Lithuania, after gaining independence, have developed at their own pace, with their own agendas and facing their own obstacles. There were many tensions accompanying a post-communist return to Europe after long years of separation and how each country responded to the demands of becoming a modern European state. Estonia was the first of the former Soviet republics to begin accession negotiations with the European Union in 1988 and is a potential candidate for the next round of EU enlargement in 2004. Lithuania and Latvia have also expressed their desire to become future members of NATO and the EU[2].

Russian interference in Western electoral processes

Russia has been accused of interfering in electoral processes in several Western countries, including in the US presidential election (2016) and elections in France and Germany. Through social media, Russian hacker groups spread fake news and polarizing narratives to influence voters and sow social discord. Russian-backed hacker groups, such as Cozy Bear and Fancy Bear, have carried out cyber-attacks on voting systems, political parties and critical infrastructure to obtain sensitive information or disrupt electoral processes. Russia's interference in Western electoral processes has been the subject of extensive research and analysis, especially after the major incidents of the 2010s. It is worth remembering the hacking of computer servers described as Watergate 2.0, where cyber thieves used everything: sensitive documents, emails, donor information, even voicemails. Western intelligence agencies traced the hack to Russian spy agencies and dubbed them “cyber bears”. Soon the media was flooded with stolen information, relayed via Julian Assange, the founder of WikiLeaks. It was a massive attack on America, but the Russian hackers seemed to have only one goal - the election of Donald J. Trump as president of the United States. Their goal? To end 240 years of free and fair American democratic elections[3]. Modern warfare is a war of narratives, where bullets are fired both physically and virtually. Whether you're a president or a terrorist, if you don't understand how to use the power of social media effectively, you may win a battle, but you will lose a 21st century war[4].

Another noteworthy example is the international intrigue, the cyber espionage, the superpower rivalry, which has led to Trump's strange relationship with Putin, the strange ties between members of his inner circle (including Paul Manafort and Michael Flynn) and Russia. That bizarre scandal explains the stakes and begets one of the biggest questions in American politics: how and why did a foreign government infiltrate the country's political process and gain influence in Washington?[5] With the end of the Cold War, the victory of liberal democracy seemed definitive. Russia had found allies among nationalists, oligarchs and radicals everywhere, and its desire to dissolve Western institutions, states and values resonated in the West itself. The rise of populism, the British vote against the EU and the election of Donald Trump were all Russian goals, but their realization reveals the vulnerability of Western societies. To understand the challenge is to see, and

[1] Anatol Lieven, *The Baltic Revolution: Estonia, Latvia and the Path to Independence*, Yale University Press, 1994, p. 17
[2] Thomas Lane, Artis Pabriks, Aldis Purs, David J. Smith, *The Baltic States: Estonia, Latvia and Lithuania*, Routledge, 2017, p. 19
[3] Malcolm Nance, *The Plot to hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*, Skyhorse, 2016, p. 77
[4] David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*, Basic Books, 2017, p. 101
[5] Michael Isikoff, Corn David, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*, Twelve, 2018, p. 13

perhaps renew, the fundamental political virtues offered by tradition and demanded by the future[1]. Examples such as poisoned dissidents, election interference, armed invasions, international treaties thrown into chaos, secret military reinforcements, hackers and viruses, weapons deployed in space are just a few examples of this conflict where certain actors are in the shadows and affected states are forced to adapt and fight back; the war of the future is already here with us[2].

Misinformation is as old as mankind. When Satan told Eve that nothing would happen if she bit the apple, that was misinformation. But the rise of social media has made disinformation even more pervasive and pernicious in our current age. In a disturbing turn of events, governments are increasingly using disinformation to create their own false narratives, and democracies are proving not very good at combating it. The information wars underline that we need to find a way to combat this growing threat to democracy[3]. We live in an age of disinformation, of organized deception. Intelligence agencies invest vast resources in hacking, leaking and falsifying data, often with the aim of weakening the very foundation of liberal democracy: trust in facts. The story of modern disinformation begins with the post-Russian Revolution confrontation between communism and capitalism that would define the Cold War. As misinformation develops, it is certain that we will live in a future of projected polarization, more active and less measured, and the tools needed to navigate through the deception[4].

The impact of hybrid warfare on the civilian population

Hybrid warfare has a profound and often devastating impact on civilians. The impact of hybrid warfare on civilians is a critical area of study that focuses on how this complex form of conflict affects populations in a variety of ways, including psychological stress, displacement and social disruption. Here's how hybrid warfare affects civilians:

Disruption of essential services

Cyber-attacks and physical attacks on critical infrastructure (electricity grids, water supplies and transportation networks) can lead to significant disruptions. These attacks often aim to cause chaos and undermine public confidence in the government. Disruption to economic activities, such as through ransomware attacks on businesses or supply chain disruptions, can lead to job losses, economic instability and increased living costs for civilians.

Spreading disinformation and propaganda

Misinformation campaigns can spread false or misleading information, creating confusion and fear among the population. Disinformation can deepen existing social divisions by promoting divisive narratives, leading to increased social polarization and fragmentation. This can damage community relations and make it more difficult to achieve social cohesion.

Psychological impact

The constant threat of cyber-attacks, disinformation and economic instability can contribute to widespread stress and anxiety among civilians. This psychological impact can be particularly severe in conflict zones or areas heavily affected by hybrid tactics. Prolonged exposure to hybrid warfare tactics, including violent incidents, disinformation and economic hardship, can lead to long-term mental health problems, including trauma, depression and PTSD (Post-traumatic stress disorder).

Impact on public services and governance

Hybrid warfare tactics such as disinformation and political subversion can erode trust in public institutions and government authorities. This can lead to decreased public confidence in the effectiveness and legitimacy of government responses. Disruption and undermining efforts can lead to weak governance, making it more difficult for governments to deliver essential services and maintain law and order. This can lead to a decline in public safety and overall quality of life.

---

[1] Timothy Snyder, *The Road to Unfreedom: Russia, Europe, America*, Crown, 2018, p. 92

[2] Jim Sciutto, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America*, Harper, 2019, p. 67

[3] Richard Stengel, *Information Wars: How We Lost the Global battle Against Disinformation and What We Can Do About It*, Atlantic Monthly Press, 2019, p. 81

[4] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, 2020, p. 17

Economic hardship

Civilians may face higher living costs due to economic disruptions such as inflation or shortages of goods and services. This can lead to financial strain, especially for vulnerable populations. Disruption to businesses and industries, including through cyber-attacks and economic sanctions, can lead to job losses and reduced economic opportunities, further affecting civilian livelihoods.

Physical safety and security

Hybrid warfare can include the use of irregular forces, terrorists and proxy groups, which can directly target civilians through attacks, bombings and other forms of violence. This can lead to casualties and displacement. Civilians in conflict or targeted areas may become more vulnerable to violence, exploitation and human rights violations. The mix of conventional and non-conventional tactics can make it harder to protect civilians.

Displacement and refugee crises

Conflict and instability resulting from hybrid wars can lead to large-scale displacement of civilians, creating refugee crises and putting pressure on neighbouring countries and international aid organizations. Displaced populations often face serious humanitarian needs, including access to shelter, food, healthcare and education. Addressing these needs can be difficult in the context of an ongoing hybrid war.

Cultural and social impact

In some cases, hybrid warfare tactics may target cultural and historical sites with the aim of eroding cultural identity and heritage. This can have lasting effects on communities and their sense of identity. The societal divisions exacerbated by hybrid warfare tactics can lead to social disintegration, making it more difficult for communities to function cohesively and support each other.

Legal and ethical implications

Tactics used in hybrid warfare can lead to various human rights violations, including arbitrary detention, torture and other forms of ill-treatment. These violations can be committed by both state and non-state actors. The combination of conventional and unconventional tactics can complicate efforts to hold perpetrators accountable, leading to a lack of justice for victims of hybrid warfare. Hybrid warfare has been an integral part of the historical landscape since antiquity, but it is only recently that analysts have incorrectly labeled these conflicts as unique. Throughout history, great powers have faced adversaries who have used a combination of regular and irregular forces to nullify the advantage of the great power's superior conventional military force. Hybrid wars are labor-intensive and long-term affairs; they are difficult battles that defy the internal logic of opinion polls and election cycles. Hybrid wars are also the most likely conflicts of the 21st century, as competitors use hybrid forces to deplete military capabilities in protracted campaigns of exhaustion[1].

Behind the physical nature of the tumult of war are structural forces that create landscapes of civilian vulnerability. These forces operate in four sectors of modern warfare: nationalist ideology, state-sponsored armies, global media and international institutions. Each sector promotes its own constructions of civilian identity in relation to militant combatants: constructions that prove lethal to non-combatant civilians who lack political power and decision-making capacity over their own survival. Civilians and Modern Warfare offers a critical perspective on the plight of civilians in war, examining the political and normative underpinnings of the decisions, actions, policies and practices of major sectors of war. The contributors seek to undermine the 'tunnel effect' of the militarist framework in terms of the experiences of non-combatants[2].

Hybrid warfare refers to a military strategy that combines conventional warfare, so-called 'irregular warfare' and cyber-attacks with other methods of influence, such as fake news, diplomacy and foreign political intervention. As hybrid warfare becomes increasingly commonplace, there is an imminent need for research to draw attention to how these challenges can be addressed to develop a comprehensive approach to hybrid threats and hybrid warfare[3].

---

[1] Williamson Murray, Peter R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012, p.75

[2] Daniel Rothbart, Karina K. Korostelina, Cherkaoui, Mohammed, *Civilians and Modern War: Armed Conflict and the Ideology of Violence (War, Conflict and Ethics)*, Routledge, 2012, p. 18

[3] Mikael Weissmann, Nikolas Nilson, Björn Palmertz, Thunholm Per, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, I. B. Tauris, 2021, p. 93

Ethics of using weapons with artificial intelligence

The ethics of AI weapons is a complex and controversial issue, involving a range of moral, legal and practical considerations. Once activated, AI weapons, often referred to as autonomous weapon systems (AWS), can operate independently of human intervention, making targeting and engagement decisions on their own. This raises several ethical issues:

Responsibility and accountability

One of the main ethical concerns is the question of liability. If an autonomous weapon causes unintentional harm, who is responsible? Is it the programmer, the manufacturer, the military commander, or the machine itself? Lack of clear accountability could lead to situations where no one is held responsible for wrongful death or destruction, undermining the principle of justice.

Human dignity and moral agency

Autonomous weapons can undermine human dignity by removing human moral agency from the decision to take life. The decision to kill has profound moral implications and many argue that it should remain under human control. Allowing machines to make life and death decisions could be considered dehumanizing and ethically unacceptable.

Distinction and proportionality

In armed conflict, the principles of distinction and proportionality are fundamental to the laws of war. Distinction requires that combatants distinguish between military targets and civilians, while proportionality requires that the harm caused by military action be proportionate to the military advantage gained. There are concerns that AI weapons may have difficulty making these complex ethical judgments, leading to indiscriminate or disproportionate attacks.

Risk of escalation

Weapons with artificial intelligence could lower the threshold for conflict, making it easier for states or non-state actors to initiate violence. The speed and efficiency of autonomous systems could lead to the rapid escalation of conflicts, reducing the time available for diplomacy and peaceful resolution. In addition, the use of AI weapons by one state could provoke an arms race as other states develop similar or more advanced systems.

Unintended consequences

Autonomous weapon systems could behave unpredictably or malfunction in ways that cause unintended harm. The complexity of artificial intelligence systems makes it difficult to foresee all possible scenarios, leading to the risk of accidents or unintended escalations. Moreover, these systems could be hacked or reused by malicious actors, which poses significant security risks.

Potential for abuse

AI weapons could be used for oppressive purposes, such as targeting political dissidents, suppressing protests or carrying out targeted assassinations without due process. The availability of such technology could allow authoritarian regimes or non-state actors to commit acts of violence with impunity, thus exacerbating human rights violations.

Legal and regulatory challenges

The development and use of AI weapons challenges existing legal frameworks, including International Humanitarian Law (IHL) and human rights law. Current legislation is not fully prepared to address the complexities of autonomous systems and there is a lack of consensus on how to regulate these weapons. Some advocate a pre-emptive ban, while others advocate stricter controls and oversight.

Ethical justifications for AI weapons

Proponents of AI weapons argue that they could reduce harm in warfare by being more accurate and effective than human soldiers. For example, AI systems could be designed to more effectively avoid collateral damage or carry out dangerous missions without risking human lives. However, these potential benefits must be balanced against significant risks and ethical challenges.

Bias and discrimination

Artificial intelligence systems are only as good as the data on which they are trained, and if that data is biased, the AI's decisions may also be biased. In the context of guns, this could lead to discriminatory targeting based on race, ethnicity or other factors. This raises serious ethical questions about fairness and the potential for AI to perpetuate or exacerbate existing injustices.

Global security and stability

The proliferation of AI weapons could destabilize global security. If more states develop and deploy such systems, this could lead to a new form of arms race, where the focus is on developing increasingly autonomous and lethal technologies. This could increase the likelihood of accidental or deliberate conflicts with potentially catastrophic consequences. AI weapons ethics is a complex and evolving topic, and several books explore it from different angles. Military robots and other potentially autonomous robotic systems such as unmanned combat aerial vehicles (UCAVs) and unmanned ground vehicles (UGVs) could soon be introduced to the battlefield. Looking further into the future, we could see autonomous micro- and nanorobots armed and deployed in swarms of thousands or even millions. This increasing automation of warfare could come to represent a major discontinuity in the history of warfare: humans will first be removed from the battlefield and one day may even be largely excluded from the decision-making cycle in the future high-tech, high-speed robotic warfare of the future. While the current technological problems will undoubtedly be overcome, the biggest obstacles to the use of automated weapons on the battlefield are likely to be legal and ethical concerns[1].

Prominent experts in science and the humanities examine aspects of robot ethics ranging from sex to war. Today, robots fulfill many roles, from entertainer to educator to executioner. As robotic technology advances, ethical concerns become more pressing: Should robots be programmed to follow an ethical code, if possible? Are there risks in forming emotional bonds with robots? How might society and ethics change with robotics? Ethics often lags technological developments[2]. The discussion on lethal autonomous weapon systems (LAWS) centers on the ethics of allowing a computer to decide to kill (or not to kill) a human being. Much of the current discourse on autonomous weapons stems from concern about the ethical implications. Efforts are currently being made to institute laws and regulations that would inhibit or eliminate the use of LAWS[3]. The ethical questions are *to what extent should such technologies be advanced*? *And if responsible democracies ban them, would they prevent rogue regimes from profiting from them*? At the forefront of a game-changing debate. When the choice is life or death, the human heart cannot be replaced[4].

Artificial intelligence is playing a growing role in military weapons systems. Going beyond the bomb-carrying drones used in the war in Afghanistan, the Pentagon is now in a race with China and Russia to develop "lethal autonomous weapon systems" (LAWS). While the use of robotic systems could reduce military casualties in a conflict, a major concern is: should we allow machines to make life-and-death decisions in combat? Other areas of concern include the following: who would be responsible for the actions of fully autonomous weapons - the programmer, the machine itself, or the country implementing LAWS? When war becomes just a matter of technology, will war become more likely, bringing humanity closer to annihilation? What will happen if artificial intelligence technology reaches a "singularity level" such that our weapons are controlled by an intelligence that surpasses human intelligence?[5]

The question of whether new rules or regulations are needed to regulate, restrict or even prohibit the use of autonomous weapon systems has been the subject of debate lately, so society needs to invest in difficult discussions that address the ethics, morality and law of these new digital technologies and understand the human role in their creation and operation[6]. Artificial intelligence is the most talked about and arguably the most powerful technology in the world today. The very rapid development of this technology and its power to change the world and perhaps even us call for a serious and systematic reflection on its ethical and social implications and on how its development should be directed[7].

Autonomous weapon systems seem to be on the way to becoming accepted technologies of war. The weaponization of artificial intelligence raises questions about the continued control of human beings over the

---

[1] Armin Krishnan Killer, *Robots: Legality and Ethicality of Autonomous Weapons*, Routledge, 2009, p. 77

[2] Patrick Lin, Keith Abney, George A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics*, The MIT Press, 2014, p. 103

[3] Ted W. Schroeder, *Lethal Autonomous Weapon Systems in Future Conflicts*, Independently Published, 2017, p. 22

[4] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company, 2018, p. 81

[5] Louis A. del Monte, *Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future of Warfare*, Prometheus, 2018, p.97

[6] Jai Galliot, Duncan MacIntosh, Jens David Ohlin, *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare (Ethics, National Security, and the Rule of Law)*, Oxford University Press, 2021, p. 89

[7] Soraj Hongladarom, *The Ethics of AI and Robotics: A Buddhist Viewpoint*, Lexington Books, 2021, p. 88

use of force. The notion of meaningful human control has become a central point of international debate on lethal autonomous weapons systems among members of the United Nations: many states have divergent ideas about various complex forms of human-machine interaction and the point at which human control ceases to be meaningful[1].

Regulating the use of autonomous weapon systems (AWS)

Regulating autonomous weapon systems (AWS) is a complex challenge that requires a multidimensional approach, involving legal, ethical, technical and international dimensions. Here are some key strategies and considerations for regulating AWS:

International legal framework

One of the main ways of regulating AWS is the establishment of new international treaties specifically addressing their development, deployment and use. Such treaties could establish clear rules and guidelines, like existing arms control agreements such as the Chemical Weapons Convention. Existing International Humanitarian Law (IHL), such as the Geneva Conventions, could be updated or reinterpreted to respond to the unique challenges posed by AWS. This could include clarifying the application of principles such as distinction, proportionality and accountability in the context of autonomous systems.

Definition and classification

A major regulatory challenge is defining what constitutes an AWS. Clear and precise definitions are essential to ensure that regulations target the systems concerned without stifling legitimate technological advances. Definitions should distinguish between different levels of autonomy and specify the characteristics that make a system subject to regulation. AWS could be categorized according to their level of autonomy, potential for harm, and intended use (e.g. lethal vs. non-lethal). This categorization could help tailor regulations to different types of systems, ensuring that the most dangerous systems are subject to the most stringent controls.

Development and testing standards

Regulations could require rigorous testing of the safety and reliability of AWS systems before they are deployed. This would involve ensuring that the systems can operate within the limits required by international law and do not pose unreasonable risks of malfunction or unintended harm. Developers of AWS should be required to document and disclose the processes used to train and test their systems, including the datasets used and the decision-making criteria. This transparency would help ensure that AWS is designed and tested with ethical considerations in mind.

Human control and supervision

Regulations could require that humans remain in the decision-making loop for critical functions, especially those involving the use of lethal force. This could involve requiring human confirmation before an AWS engages a target. Even for systems that operate autonomously, mechanisms should be in place to ensure human oversight and accountability. Regulations could specify who is responsible for the actions of an AWS, including the roles of commanders, operators and developers.

Ethical guidelines and codes of conduct

Governments, international organizations and industry groups could develop ethical frameworks to guide the development and use of AWS. These could include principles such as respect for human dignity, the need to minimize harm, and the importance of maintaining human control over critical decisions. AWS developers and operators could be required to adhere to codes of conduct that align with these ethical frameworks. These codes could include commitments to transparency, accountability and avoid civilian harm.

International cooperation and standards

Some proponents propose a global moratorium on the development and deployment of AWS until a comprehensive regulatory framework is in place. This would prevent a potential arms race and allow time for international discussions on how best to regulate these systems. To build confidence and prevent escalations, States could engage in confidence-building measures, such as sharing information on their AWS programs, participating in joint exercises, and engaging in mutual verification processes.

Export control and non-proliferation

[1] Hendrik Huelss, Ingvild Bode, *Autonomous Weapons Systems and International Norms*, McGill-Queen′s University Press, 2022, p. 84

Regulations could impose strict controls on the export of AWS and related technologies, especially to conflict regions or actors with a poor human rights record. This would help prevent proliferation of these systems to irresponsible or dangerous parties. States could negotiate non-proliferation agreements that limit the spread of AWS technologies and prevent their use in violation of international law.

Public and stakeholder involvement

Governments and international bodies should work with the public, civil society and experts in AI, ethics and international law to gather input on VAS regulation. Public consultation can help ensure that regulations reflect societal values and concerns. Regulation should involve collaboration between governments, the private sector, academia and civil society. This multi-stakeholder approach can help ensure that regulations are based on diverse perspectives and expertise.

Liability mechanisms

The regulations should establish clear mechanisms of legal liability for the use of AWS. These could include provisions for holding individuals or entities legally liable for unlawful use of AWS, whether through criminal prosecution, civil liability or other legal means. Some have proposed the creation of an international tribunal or special oversight body for AWS-related incidents. This body could investigate alleged violations of international law and provide a forum for dispute resolution.

Research and development safeguards

Institutions involved in AWS research and development could be required to establish ethical review boards to assess the potential impact of their work. These panels could ensure that R&D activities comply with ethical standards and do not contribute to the development of harmful or illegal technologies. Regulation should address the dual-use nature of AI technologies, which can be used for both civilian and military purposes. There should be safeguards to prevent the misuse of AI research for the development of autonomous weapons. Regulating autonomous weapon systems (AWS) is a crucial and complex topic. Artificial intelligence helps you choose what books you buy, what movies you see and even who you date. It puts "intelligence" into your smartphone and will soon be driving your car. But artificial intelligence could also threaten our very existence. Scientists argue that once artificial intelligence reaches this level, it will have survival needs like ours. We could be forced to compete with a rival more cunning, powerful and alien than we can imagine[1].

Stories about unmanned vehicles are now regularly in the national news, and not always in a good way. When utilized in military operations, autonomous weapon systems (AWS) have the potential to save lives as well as apply lethal force on land, at sea and in the air. The development of AWS policy and doctrine should characterize autonomy not as a discrete property of a particular system, but rather as a function that varies with the strategic, operational and tactical context and mission application. AWS design, planning, and operations should be tempered by intentional consideration of human judgment and control, as well as legal and ethical standards that promote international credibility[2].

Over the past decade, armed drones have entered the military arsenal as a basic tactic to combat terrorism. When combined with access to reliable intelligence, they make it possible to deploy a lethal force accurately across borders while keeping your own soldiers out of harm's way. The ability to direct force with great precision also offers the possibility of reducing civilian harm. At the same time, because drones remove some of the traditional constraints on the use of force, such as the need to gain political support for full mobilization, they lower the threshold for launching military strikes. The development of drone capabilities in dozens of countries increases the need for global standards on the use of these weapons to ensure that their use is strategically wise and ethically and legally sound[3].

[1] James Barrar, *Our Final Intervention: Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013, p. 79

[2] Jeffrey L. Caton, *Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues*, 2015, p. 53

[3] David R. T. Gardner, *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, University of Chicago Press, 2015, p. 97

The future of artificial intelligence ethics

The future of AI ethics is poised to become increasingly critical as artificial intelligence continues to evolve and integrate more deeply into society. Here are some key trends and considerations that will likely shape the future of AI ethics:

Evolution of ethical frameworks

As AI systems become more advanced and are used in a wider range of contexts, ethical frameworks will need to evolve dynamically. These frameworks need to adapt to new applications, societal changes and cultural differences. Ethical considerations will increasingly need to consider the specific contexts in which AI is used, such as healthcare, law enforcement, finance and privacy. The future of AI ethics will involve greater collaboration between ethicists, technologists, policy makers and other stakeholders. Inter-disciplinary approaches will be essential to address the complex ethical challenges raised by AI, ensuring the integration of ethical considerations throughout the AI development process.

IA governance and regulation

The development of international standards and agreements will be essential to regulate the ethical use of AI across borders. This could involve the creation of global regulatory bodies or agreements that establish basic ethical standards and best practices for the development and implementation of AI. AI regulation will need to be responsive and adaptive to keep pace with technological advances. This could involve the use of regulatory sandboxes where new AI technologies can be tested in a controlled environment, allowing regulators to better understand their implications and refine regulation accordingly.

The ethics of artificial intelligence in decision-making

As AI systems increasingly make decisions that have an impact on people's lives, there will be a growing emphasis on transparency and explainability. People affected by AI-driven decisions will demand to know how those decisions are made and ensuring that AI systems are interpretable will become a key ethical priority. Addressing bias and ensuring fairness in AI decision-making will remain a central ethical challenge. Future efforts are likely to focus on developing more sophisticated techniques to detect, mitigate and prevent bias in AI systems, as well as on ensuring that AI-based decisions do not perpetuate or exacerbate social inequalities.

Ethical AI in the workforce

As AI continues to automate tasks and transform industries, ethical considerations related to the impact on employment will become more pressing. Policymakers and businesses will need to address issues such as job displacement, retraining, and the creation of new opportunities to ensure that the benefits of AI are distributed. The future of work will increasingly involve collaboration between humans and AI. Ethical guidelines will be needed to ensure that this collaboration respects human dignity, promotes worker autonomy, and does not lead to exploitation or over-reliance on AI systems.

AI and privacy

As AI systems rely heavily on data, ensuring the collection, use and ethical protection of personal data will be a key concern. Future ethical frameworks will need to address issues of consent, data ownership and the potential for AI to infringe on individual privacy rights. The use of AI in surveillance raises significant ethical issues, particularly in relation to privacy, autonomy and potential misuse by governments or corporations. Balancing the benefits of AI-based surveillance with the need to protect civil liberties will be an ongoing ethical challenge.

Ethics of autonomous systems

The ethical implications of autonomous weapons will continue to be a major topic of debate. The future is likely to see increased efforts to regulate or even ban these systems, with a focus on ensuring that decisions to use lethal force remain under human control. As autonomous vehicles and other artificial intelligence systems become more prevalent in public spaces, ethical considerations will need to address issues such as safety, liability, and impact on public infrastructure. Ensuring that these systems operate safely and fairly will be a priority.

AI and the ethical development of AI

Future AI ethics will increasingly focus on integrating ethical considerations directly into the design and development of AI systems. This could involve the use of ethical impact assessments, incorporating ethical principles into AI algorithms, and adopting design practices that prioritize the welfare of the user and the good of society. Companies developing AI technologies will face increasing pressure to adhere to ethical standards

and demonstrate their commitment to responsible AI practices. This could include transparency in AI development, accountability for AI-related harms and efforts to ensure that AI benefits society as a whole.

AI and human rights

AI has the potential to exacerbate existing inequalities, and future ethical frameworks will need to address the impact of AI on marginalized and vulnerable populations. This could involve ensuring that AI systems are inclusive, do not discriminate and contribute to social justice. The use of AI in areas such as surveillance, predictive policing and social scoring systems pose significant threats to individual freedoms and human rights. The ethical development of AI will need to prioritize the protection of human rights and the prevention of the use of AI as a tool of oppression.

Ethics of artificial intelligence in healthcare

As AI is increasingly used in healthcare for diagnostics, treatment planning and personalized medicine, ethical considerations related to patient confidentiality and informed consent will become more important. Ensuring that AI-based healthcare respects patient autonomy and confidentiality will be essential. AI has the potential to improve healthcare outcomes, but risks widening disparities in access to care. Ethical frameworks will need to address how AI can be used to promote equitable access to care and improve outcomes for all patients.

Public involvement and education

The future of AI ethics will involve greater efforts to engage the public in discussions about the ethical implications of AI. This includes educating people about how AI systems work, the potential risks and benefits, and their rights in an AI-driven world. It will be important to ensure that the development of AI ethics is inclusive and reflects diverse perspectives. This could involve creating platforms for public input, ensuring that underrepresented voices are heard and promoting a more democratic approach to AI governance.

Exploring the future of AI ethics is a fascinating and crucial area of study given the rapid advances in AI technologies. In the popular imagination, superhuman artificial intelligence is a coming wave that threatens not just human jobs and relationships, but civilization itself. Conflict between humans and machines is seen as inevitable, and its outcome is all too predictable[1]. What is certain is that we will all need to understand the enormous potential of artificial intelligence to transform our daily lives, but also how our lives will be shaped by artificial intelligence[2].

The impact of artificial intelligence on hybrid conflicts in the 21st century

Artificial Intelligence (AI) has significantly influenced hybrid conflicts in the 21st century, with both advantages and disadvantages. Hybrid conflicts are complex, involving a mix of conventional military tactics, irregular warfare, cyber operations and political subversion. We are just beginning to see a massive change in military technology. As these technologies proliferate, they will have profound effects both on the front line and on politics at home. Removing humans from the battlefield makes wars easier to start but more complex to fight. Replacing men with machines may save some lives but will reduce morale and psychological barriers to killing. The "warrior ethic" that has long defined the identity of soldiers will erode, as will the laws of war that have governed military conflicts for generations. Paradoxically, these new technologies will bring war to our doorstep. The future of war is as fascinating as it is terrifying[3]. Due to unprecedented developments in artificial intelligence, dramatic changes will take place much sooner than many of us expected. Most experts are already saying that AI will have a devastating impact on jobs for workers. The jobs that will be affected and over how long, the jobs that can be improved with AI and, most importantly, how we can provide solutions to some of the most profound changes in the future of human history[4]. The heady optimism of the early days of the internet has turned dark. The fight for a humane future has never been more urgent. We still have the power to decide what kind of world we want to live in[5].

[1] Stuart Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, 2019, p. 66
[2] Kai-Fu Lee, Chen Quifan, *AI 2041: Ten Visions for Our Future*, Crown Currency, 2021, p. 37
[3] Peter Singer, *Warren, Wired for War: The Robotics revolution and Conflict in the 21st Century*, Penguin Books, 2009, p. 67
[4] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, Harper Business, 2018, p. 57
[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, p. 79

As a general-purpose and dual-purpose technology, artificial intelligence can be used for both good and bad. The use of artificial intelligence is becoming increasingly important to the government's mission to keep its nations safe. However, the design, development and use of AI for national security raises a wide range of legal, ethical, moral and privacy issues. In examining the contradictory uses of AI, some countries use AI to launch disinformation attacks by automating the creation of false or misleading information to undermine public discourse[1].

1. Advantages of using artificial intelligence in hybrid conflicts

Enhanced surveillance and intelligence gathering

Artificial intelligence can process large amounts of data from various sources, such as social media, satellite imagery and communication intercepts, to identify patterns and potential threats. This helps in taking preventive measures and situational awareness. AI models can predict enemy movements and intentions by analyzing historical data and current trends, thus improving strategic planning.

Improved cyber capabilities

AI systems can automatically detect and respond to cyber threats, strengthening defenses against hacking and cyber-espionage. Artificial intelligence can be used to develop sophisticated malware or execute cyber-attacks with high precision, disrupting adversaries' communications and infrastructure.

Autonomous systems

Artificial intelligence-powered drones and robotic systems can perform reconnaissance, deliver payloads or engage in combat with minimal human intervention, reducing the risk to personnel. AI can optimize logistics and supply chains, improving the efficiency of military operations and resource allocation.

Enhanced information warfare

AI can rapidly generate and spread disinformation, influencing public opinion and destabilizing societies. This can be used to manipulate perceptions and sow discord among adversaries. AI algorithms can amplify certain narratives or suppress others, shaping the information environment in favor of one side.

2. Disadvantages of artificial intelligence in hybrid conflicts

Ethical and legal concerns

The use of AI in autonomous weapons raises ethical concerns such as the potential for unintended escalation and lack of accountability for actions taken by machines. AI-based operations, particularly in cyber warfare, can unintentionally damage civilian infrastructure, leading to collateral damage and humanitarian crises.

Vulnerability to AI manipulation

AI systems themselves can be vulnerable to adversarial attacks, where slight manipulations of input data can cause the AI to make incorrect decisions or predictions.AI systems can inherit biases from their training data, which can lead to faulty intelligence and decision making.

Escalation risks

The speed and scale at which artificial intelligence can operate could lead to the rapid escalation of conflicts, as automated systems can act faster than human surveillance can manage. The development of advanced artificial intelligence in military applications may trigger an arms race, with nations competing to outdo each other in artificial intelligence capabilities, increasing global tensions.

Over-reliance and over-reliance

Over-reliance on AI systems can lead to vulnerabilities if these systems malfunction or are compromised. Human oversight is essential to mitigate these risks. Over-reliance on artificial intelligence could erode human judgment and critical decision-making, leading to less adaptive responses in unpredictable situations.

In short, while AI offers significant advantages in improving capabilities and effectiveness in hybrid conflicts, it also introduces new risks and ethical dilemmas. Balancing the benefits with the potential drawbacks is essential to ensure that AI contributes positively to security and stability, rather than exacerbating conflict.

[1] Reza Montasari, *Artificial Intelligence and national Security*, Springer, 2022, p. 91

International law rules for and against the use of artificial intelligence in hybrid conflicts in the 21st century

International law on the use of artificial intelligence (AI) in hybrid conflict is still developing, reflecting the rapidly evolving nature of the technology and its application in military and non-military domains. There are aspects of existing international law that can be interpreted as favorable or restrictive to the use of AI in such contexts. Here is a breakdown of these perspectives:

Existing legal frameworks supporting the use of AI

· Principle of state sovereignty and self-defense:

Article 51 of the UN Charter. This article allows states the right to self-defense if they are attacked. AI-driven defensive systems, such as automated cybersecurity measures, can be considered legitimate tools for protecting a nation's infrastructure.

Law of Armed Conflict (LOAC)/International Humanitarian Law (IHL). AI technologies that comply with the principles of LOAC, such as distinction (differentiating between combatants and non-combatants) and proportionality (ensuring that harm to civilians is minimized), may be permitted. For example, AI could be used for improved targeting and reduced collateral damage in military operations.

· Cybersecurity and defense norms:

Tallinn Manual on the International Law Applicable to Cyber Warfare. While not legally binding, this manual provides guidance on how existing international law might apply to cyber operations, including the use of AI. It suggests that states can use AI for cyber defense as long as it respects the norms of sovereignty and proportionality.

Legal and ethical constraints on the use of AI

· Geneva Conventions:

The Geneva Conventions and their Additional Protocols regulate conduct during armed conflicts, emphasizing the protection of civilians. AI systems used in warfare must comply with these conventions by ensuring they can distinguish between legitimate military targets and protected civilians.

Article 36 of Additional Protocol I. Requires states to review new weapons, methods, or means of warfare to ensure they are not prohibited by international law. This would apply to autonomous AI systems and lethal autonomous weapon systems (LAWS).

· Human rights law:

International Covenant on Civil and Political Rights (ICCPR). Ensures the right to life and prohibits arbitrary deprivation of life. The use of AI in hybrid conflicts, especially in autonomous weapons systems, must be designed and used in a way that upholds these principles.

· Ethical constraints on autonomous systems:

"Meaningful Human Control" Doctrine. Many international bodies, including the UN and advocacy groups, argue that any AI system capable of lethal action should operate under meaningful human oversight. The use of AI in decision-making without human control raises serious ethical and legal concerns.

UN Group of Governmental Experts on LAWS. This group has discussed the implications of autonomous weaponry, recommending restrictions to ensure that humans remain responsible for life-or-death decisions.

Potential Violations and Concerns

·Accountability and attribution.

One of the primary concerns is how to attribute responsibility for actions taken by AI systems. If an autonomous AI system acts outside the bounds of international law or commits an unlawful act, it can be difficult to determine who is legally accountable—the state, the manufacturer, or the operator.

·Discrimination and bias:

AI systems can inherit biases from their training data, leading to potential discrimination in targeting or operational errors. This can violate the principle of distinction and potentially result in disproportionate harm to civilians.

·Cyber operations and AI:

The use of AI in cyber-attacks poses legal challenges regarding sovereignty and the prohibition against non-consensual interference in the internal affairs of states (Article 2(4) of the UN Charter). AI-driven cyber operations that result in significant damage to a state's infrastructure or economy may be considered an act of aggression.

International Calls for Regulation

·UN and International Advocacy:

The United Nations, through various arms such as the UN Institute for Disarmament Research (UNIDIR), has called for discussions around AI and autonomous systems, promoting international norms and possibly new treaties to regulate their use.

·Campaign to Stop Killer Robots:

This international coalition advocates for a preemptive ban on fully autonomous weapons to ensure that decisions involving the use of force remain under human control.

·Global Partnership on AI (GPAI):

GPAI is an international initiative aimed at responsible AI use. Although not directly related to hybrid warfare, it promotes guidelines that can influence the development and use of AI in defense.

Emerging Legal and Policy Gaps

·Absence of Specific Treaties:

Currently, there is no binding international treaty specifically regulating the use of AI in hybrid conflicts. The laws that do apply are extrapolated from general principles of international humanitarian and human rights law.

·Rapid Technological Advancements:

The pace of AI development often outstrips the creation and implementation of laws and regulations. This creates a gap where states and non-state actors can leverage AI in ways that may not yet be fully addressed by existing legal frameworks.

Although international law provides some structure for the use of AI in conflict through general principles of international humanitarian law and human rights law, significant legal and regulatory gaps remain, particularly in the areas of accountability, the use of lethal autonomous systems and cyber operations. Efforts to establish new treaties or agreements specific to AI and hybrid warfare are ongoing, but the international community faces challenges in keeping pace with rapid technological advances.

Bibliography

Books

1. Altunisik, Meliha; Tur, Ozlem, *Turkey: Challenges of Continuity and Change*, Routledge, 2022
2. Applebaum, Anne, *Red Famine: Stalin's War on Ukraine*, Doubleday, 2017
3. Asmus, Ronald, *Little War That Shook the World: Georgia, Russia, and the Future of the West*, St. Martin′s Press, 2010
4. Bajoghli, Narges, *Iran Reframed: Anxieties of Power in the Islamic Republic*, Stanford University Press, 2019
5. Barkey, Henry, J., *Reluctant Neighbor: Turkey's Role in the Middle East*, United States Institute of Peace, 1997
6. Barrar, James, *Our Final Intervention: Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013
7. Barto, Andrew, G.; Sutton, Richard, S., *Reinforcement Learning: An Introduction*, Bradford Books, 2018
8. Beebe, George, *The Russia Trap: How Our Shadow War with Russia Could Spiral into Catastrophe*, Thomas Dunne, 2019
9. Berman, Ilan; Humire, Joseph, M., *Iran's Strategic Penetration of Latin America*, Lexington Books, 2016
10. Bostrom, Nick, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2016
11. Caton, Jeffrey, L., *Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues*, lulu.com, 2015
12. Coeckelbergh, Mark, *AI Ethics*, The MIT Press, 2020
13. Cornell, Svante, E.; Starr, Frederick, S., *The Guns of August 2008: Russia's War in Georgia*, Routledge, 2009
14. Corr, Andreas, *Great Powers, Grand Strategies: The New Game in the South China Sea*, Naval Institute Press, 2018
15. Crist, David, *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran*, Penguin Publishing Group, 2013

16. de Wall, Thomas, *The Caucasus: An Introduction*, Oxford University Press, 2010
17. Demir, Ýdris, *Turkey's Foreign Policy Towards the Middle East: Under the Shadow of the Arab*, Cambridge Scholars Publishing, 2016
18. Dewan, Sandeep, *China's Maritime Ambitions and the PLA Navy*, Vij Books India, 2013
19. Erickson, Andrew, S.; Goldstein, Lyle, J.; Li, Nan, *China, the United States, and 21st-Century Sea Power: Defining a maritime Security Partnership*, Naval Institute Press, 2010
20. Freedman, Lawrence, *Ukraine and the Art of Strategy*, Oxford University Press, 2019
21. Galeotti, Mark, *Putin's Wars: From Chechnya to Ukraine*, Osprey Publishing, 2022
22. Galliot, Jai; MacIntosh, Duncan; Ohlin, Jens, David, *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare (Ethics, National Security, and the Rule of Law)*, Oxford University Press, 2021
23. Gardner, David, R., T., *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, University of Chicago Press, 2015
24. Géron, Aurélien, *Hands-On Machine Learning with Scikit-Learn, Keras, And TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O′Reilly Media, 2019
25. Goodfellow, Ian; Bengio, Yoshua, Courville, *Deep Learning*, The MIT Press, 2016
26. Hayton, Bill, *The South China Sea: The Struggle for Power in Asia*, Yale University Press, 2014
27. Hongladarom, Soraj, *The Ethics of AI and Robotics: A Buddhist Viewpoint*, Lexington Books, 2021
28. Huelss, Hendrik; Bode, Ingvild, *Autonomous Weapons Systems and International Norms*, McGill-Queen′s University Press, 2022
29. Işikal, Hüseyin; Göksel, Oğuzhan, *Turkey's Relations with the Middle East: Political Encounters after the Arab Spring*, Springer, 2018
30. Isikoff, Michael; Corn, David, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*, Twelve, 2018
31. Jones, Stephen, F., *Georgia: A Political History Since Independence*, I. B. Tauris, 2012
32. Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2017
33. Kaplan, Robert, D., *Asia's Cauldron: The South China and the End of a Stable Pacific*, Random House Trade Papperbacks, 2015
34. Kösebalaban, Hasan, *Turkish Foreign Policy: Islam, Nationalism, and Globalization (Middle East Today)*, Palgrave Macmillan, 2011
35. Krishnan, Armin, *Killer Robots: Legality and Ethicality of Autonomous Weapons*, Routledge, 2009
36. Lane, Thomas; Pabriks, Artis; Purs, Aldis; Smith, David, J., *The Baltic States: Estonia, Latvia and Lithuania*, Routledge, 2017
37. Lee, Kai-Fu, *AI Superpowers: China, Silicon Valley, and the New World Order*, Harper Business, 2018
38. Lee, Kai-Fu, Quifan, Chen, *AI 2041: Ten Visions for Our Future*, Crown Currency, 2021
39. Lieven, Anatol, *The Baltic Revolution: Estonia, Latvia and the Path to Independence*, Yale University Press, 1994
40. Lin, Patrick; Abney, Keith; Bekey, George, A., *Robot Ethics: The Ethical and Social Implications of Robotics*, The MIT Press, 2014
41. Melamed, Avi, *Inside the Middle East: Making Sense of the Most Dangerous and Complicated Region on Earth*, Skyhorse, 2016
42. Miller, Christopher, *The War Came To Us: Life and Death in Ukraine*, Bloomsbury Continuum, 2023
43. Mitchell, Melanie, *Artificial Intelligence: A Guide for Thinking Human*. Farrar, Straus and Giroux, 2019
44. Montasari, Reza, *Artificial Intelligence and national Security*, Springer, 2022
45. Murray, Williamson, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012
46. Murray, Williamson; Mansoor, Peter, R., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012
47. Nance, Malcolm, *The Plot to hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*, Skyhorse, 2016
48. Nasr, Vali, *The Shia Revival: How Conflicts within Islam Will Shape the Future*, W W Norton & Co Inc, 2007

49. Öniș, Ziya; Keyman, Fuat, E., *Turkish Politics in a Changing World: Global Dynamics and Domestic Transformations*, Istanbul Bilgi University Yayinlari, 2007
50. Patrikarakos, David, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*, Basic Books, 2017
51. Plokhy, Serhii, *The Gates of Europe: A History of Ukraine*, Basic Books, 2017
52. Rid, Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, 2020
53. Rothbart, Daniel; Korostelina, Karina, K.; Cherkaoui, Mohammed, *Civilians and Modern War: Armed Conflict and the Ideology of Violence (War, Conflict and Ethics*), Routledge, 2012
54. Russell, Stuart, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, 2019
55. Scharre, Paul, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton&Company, 2018
56. Schroeder, Ted, W., *Lethal Autonomous Weapon Systems in Future Conflicts*, Independently published, 2017
57. Sciutto, Jim, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America*, Harper, 2019
58. Shirreff, Richard, *War with Russia: An Urgent Warning from Senior Military Command*, Quercus, 2016
59. Snyder, Timothy, *The Road to Unfreedom: Russia, Europe, America*, Crown, 2018
60. Stengel, Richard, *Information Wars: How We Lost the Global battle Against Disinformation and What We Can Do About It*, Atlantic Monthly Press, 2019
61. Stryker, Cole, *Hacking the Future: Privacy, Identity, and Anonymity on the Web*, Abrams Press, 2012
62. Weissmann, Mikael; Nilson, Nikolas; Palmertz, Björn; Thunholm, Per, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, I. B. Tauris, 2021
63. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019

Éva JAKUSNÉ HARNOS
Ludovika University of Public Service, Hungary

WHOSE STRATEGIC NARRATIVE? THE IMPACT OF DIGITAL TECHNOLOGY ON SOCIETAL SECURITY

Abstract:	*Strategic narratives are descriptions and interpretations of events of the world from the perspective of agents in international relations. They offer a justification for the agent's actions and ambitions and ensure cohesion and support within the agent's community. The article shortly summarises major changes caused by modern technology in the formation and projection of strategic narratives, then discusses reception in detail. In the investigation of strategic narratives, projection got into the focus at the beginning of the digital age and only recently has attention turned towards reception, that is, impact on society.* *The theoretical background of societal security originating from the Copenhagen School allows an overview of the vulnerabilities of modern communities to disinformation, also highlighting the trans-sectoral nature of the threats. The conclusion of the paper is that modern liberal democracies are at a disadvantage in developing protection against disinformation because of their fundamental values. The privatization of media outlets was welcomed a few decades ago and the concentration of media ownership was not deemed dangerous. However, if media is securitized, the increase of control may be necessary, otherwise maintaining cohesion through one's own strategic narrative and blocking rival strategic narrative may become impossible.*
Keywords:	**Strategic narrative; societal security; media landscape; identity; ideology**
Contact details of the authors:	E-mail: Jakusne.Harnos.Eva@uni-nke.hu
Institutional affiliation of the authors:	**Ludovika University of Public Service, Hungary**
Institutions address:	Ludovika tér 2, Budapest, 1083; https://www.uni-nke.hu/

Introduction

Our era is often characterised by the intensification of strategic competition among status quo and revisionist powers, with the latter aspiring to take a new position in the international arena as new poles. The outcome of this struggle would be a multi-polar world. The processes are marked by the appearance of advanced technologies, especially digital technologies, which allow reaching target audiences better than before, also amplifying voices in both the conventional news media and social media. Beside the global power shift, various agents try to impact the public: not only states but also non-state actors, for example, international organisations, multi-national corporations and non-governmental organisations, and diverse lobby groups, secret agencies, extremist organisations, just to mention a few.

This article focuses on strategic narratives which contain descriptions and interpretations of events of the world from the perspective of agents in international relations. They offer a justification for the agent's actions and ambitions and ensure cohesion and support within the agent's community. Narratives allocate meaning to past, present or future events and represent perceived interests. Zaffran[1] categorizes strategic narratives into three types: system narratives (about the international order), identity narratives (agents or actors in the international system) and policy narratives (justifying specific policies or action). Narratives can be described as a kind of storytelling, during which the seemingly unrelated facts of reality are organised into a

[1] Raphael Zaffran, *Strategic Narrative and Security*, in Bryan Taylor, Hamilton Bean (Eds.), *The Handbook of Communication and Security*, Routledge, Taylor and Francis Group, New York, London, 2019, p. 354

"plot" having the structure of any narrative in human history: there is a complication emerging against the background of settings, which is eliminated, and order is restored or created as a result of action. Journalists trained by the classical standards of their profession know that news stories are the best disseminators of information and pass on the evaluation of that information. Although the latter is termed media framing nowadays, which hides the fact that, traditionally, evaluation is always included, what is more, is an obligatory element.

Narratives display structures of attention by bringing to the foreground certain aspects of reality while ignoring others. Besides, they construct chronologies, cause and effect relationships, means and ends links, thus making sense of the flow of information confusing to ordinary people. In summary, narratives create identity to which interests and values can be connected and on which cohesion can be founded[1].

This analysis centres on the following research questions: 1. What changes have occurred in the production of strategic narratives in the digital era? 2. How does the interference of opposing strategic narratives impact societal security? To answer these questions, I will investigate the interrelationship between ideology, persuasion and strategic narrative. Then I will summarise the changes in the formation, projection and reception of strategic narratives in the age of the internet. The theoretical background of societal security originating from the Copenhagen School allows an overview of the vulnerabilities of modern communities to disinformation. The theory of securitization provides a methodological framework for analysing a case study on banning media outlets during the Russia−Ukraine war. Finally, I will highlight the trans-sectoral nature of the threats coming from the modern media landscape.

The link between ideology and strategic narrative

The (political) objectives of actors are mostly supported by seemingly scientific theories, ideologies, which are disseminated by strategic narratives.[2] Ideology provides orientation and goal, which often manifests in the description of ideal end-states. Ideology is a set of beliefs, presented as a coherent world view that shapes norms and attitudes in society, leading to behaviour which is desirable for its propagator. It determines what is acceptable, right or wrong in a particular context[3]. Ideology always manifests in political discourse on certain focus topics and concepts and has a regulatory impact on behaviour. Thus, the prominence of dominant political discourse in international relations is obvious: it sets the agenda, focuses or distracts attention and influences agents in their actions.

In this article the term strategic narrative is used as the storytelling segment of political discourse, which describes the world from the perspective of a specific actor in international relations. This explains the importance of the media: the agents who have access to greater publicity will have more efficient communication. The prevalent political discourse always seems obvious to people who are surrounded by it, and discourse which diverts because it represents different ideologies is noticed and identified as an attempt at persuasion.

Research into strategic narratives

One way of the academic research of strategic narratives is segmenting their operation into formation, projection and reception[4]. Research into formation is as old as history, taking into consideration the history of propaganda and a recent classification of forms of organised persuasive communication (OPC)[5].

It is known that the term "propaganda" has been discredited due to manipulation during the world wars, however, its definition could still be used as an umbrella term for all types of persuasion: it is "a deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behaviour to achieve a

[1] Andreas Antoniades, Alister; Miskimmon, Ben O'Loughlin, *Great Power Politics and Strategic Narratives*, "CGPE", University of Sussex, Working Paper No. 7, 2010, p. 5, https://www.sussex.ac.uk/webteam/gateway/file.php?name=cgpe-wp07-antoniades-miskimmon-oloughlin.pdf&site=359 (21.11.2024)

[2] Alister Miskimmon, Ben O'Loughlin, Laura Roselle, *Forging the World: Strategic Narratives and International Relations*, University of Michigan Press, 2017, https://www.jstor.org/stable/10.3998/mpub.6504652 (21.11.2024)

[3] Garth S. Jowett, Victoria J. O'Donnell, *Propaganda and Persuasion*. SAGE Publications, 2015, p. 315

[4] Andreas Antoniades, Alister Miskimmon, Ben O'Loughlin, *Op. cit.* p. 5

[5] Vian Bakir, Eric Herring, David Miller, Piers Robinson, *Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture*, "Critical Sociology", Vol. 45, No. 3, 2018, p. 311−328, DOI: 10.1177/0896920518764586 (21.11.2024)

response that furthers the desired intent of the propagandist"[1]. To avoid using the word "propaganda", and to systemize its variations, Bakir et al.[2] coined the phrase organised persuasive communication (OPC) and placed its types along a scale. They argue that the academic study of persuasion is only possible if we recognise that persuasive communication permeates all fields of life in any political system, and it is the degree of transparency that distinguishes acceptable forms from unacceptable ones.

After the end of the Cold War, the concept of public diplomacy became widely used, comprising five areas: listening, advocacy, cultural diplomacy, exchange diplomacy and international broadcasting[3]. Obviously, international broadcasting involved the dissemination of state-sponsored news favourable to the objectives of the stakeholder, that is, of strategic narrative designed from their perspective[4]. Public diplomacy is an area of exercising soft power, which is defined as the ability of a country to attract others, especially with one's culture and values, which may result in an ability to manipulate the agenda of political choices available to others[5]. It appears that, by now, the transparent and regulated operation of public diplomacy conveying positive messages has nearly disappeared and has been replaced by mostly negative messages included in fake news campaigns trying to degrade rivals and intimidate their possible supporters.

Deceptive and fake news campaigns are against the norms of Western journalism and international cooperation, so the fact that digital technology has created a grey zone regarding legal regulations, the standards of maintaining international relations and managing home affairs has led to increased efforts to conceal sources, perspectives, stakeholders and media responsibility. The result is twofold: first, institutionalised news production has experienced upheavals, and the boundaries of professional news industry and social media communication have become blurred[6]. For example, social media posts and videos are routinely used in professional news reports. They are usually embedded in articles created by professionals to give credit to the information and deliver a sense of up-to-datedness. These also suggest inclusion, that citizens can take part in news reporting. Obviously, it is thought to make "conventional" news reporting more interactive and more like social media communication, which is considered a rival. Second, genres (i.e., types of texts) have merged and offer no clue to news consumers about source and quality. The resulting outcomes regarding strategic narratives are as follows.

Changes in formation. The location of international broadcasting in the framework of public diplomacy underscores the importance of news production, even though much of it seems to be out of state control in the era of corporate news production and of social media[7]. In addition, the amount of content from social media coming from concealed or disguised sources is on the increase. Legal regulation and the adjustment of journalistic rules are always delayed in comparison to technological innovations.

Changes in projection. Extensive academic literature discusses the effect and efficiency of targeted communication on digital devices. This technology is available to any of the competing sides, along with forms of deception enhanced by the technology itself. Profiling allows locking individual users into opinion (or (dis)information) bubbles, and digital technology, along with artificial intelligence can falsify a message and its context to make it seemingly credible. The reliance on the persuasive impact of visual images offers a broad area of future research into the psychological impact of self-persuasion as well as the evasion of responsibility by sources which exploit the opportunity lying in the "grey zone" transformation of news production.

Changes in reception. Target audience can be citizens of an actor's own country or citizens of another state. This means that alien strategic narratives mixed into the usual political discourse of a community may impact masses of people within a short time, the result of which can be "hijacking" the majority opinion at least temporarily, while the source of misleading information remains hidden to the community. If the source

[1] Garth S. Jowett, Victoria J. O'Donnell, *Propaganda and Persuasion*, SAGE Publications, 2015, p. 7
[2] *Idem*
[3] Nicholas J. Cull, *Public Diplomacy: Taxonomies and Histories*, "The Annals of the American Academy of Political and Social Science", Vol. 616, Public Diplomacy in a Changing World, March 2008, p. 32
[4] *Idem*
[5] Joseph S. Nye, *Soft Power: The Means to Success in World Politics*, Public Affairs, New York, 2004, p. 7
[6] Udo Fink, Inez Gillich, *Fake News as a Challenge for Journalistic Standards in Modern Democracy*, "University of Louisville Law Review", Vol. 58, No. 2, Spring 2020, pp. 263-282
[7] Monroe E. Price, Susan Haas, Drew Margolin, *New Technologies and International Broadcasting: Reflections on Adaptations and Transformations*, "The Annals of the American Academy of Political and Social Science", Vol. 616, Public Diplomacy in a Changing World, March 2008, pp.150-172

is not recognised, the related interests are not detected either. Citizens will not realise their self-persuasion, instead, they will believe the alien perspective and attitude are their own. The outcome may be not only action, which is not founded on informed and responsible decision, but even a shift in identity.

The impact of opposing strategic narratives on societal security

The discussion of examples of securitization and references to securitization theory usually emphasize the role of the media in the persuasion of society that a phenomenon is an existential threat and requires emergency measures even though they may infringe democratic freedoms. In modern democracies the securitization of the media, that is, of news production and consumption seems a taboo except for an armed conflict or war. For example, among the first measures in response to the Russian military aggression against Ukraine, the European Union "urgently suspended" Russia Today and Sputnik broadcast in its member states on 2 March in 2022[1] because it found that the Russian Federation "engaged in a systematic, international campaign of disinformation, information manipulation and distortion of facts in order to enhance its strategy of destabilisation of its neighbouring countries, the EU and its member states". As it was mentioned in the previous section, rival or enemy strategic narratives may influence identity, so the significance of identity in the societal sector of security needs examination. In their classic book, Buzan, Weaver and de Wilde describe their sectoral concept of security, which includes societal security[2]. They highlight that identity is the most important organizing concept in the societal sector of security, and communities construct their identity by contrasting "we", that is, the in-group, and "they", that is, the out-group. The integration of groups in the society takes place through common culture and its reproduction processes (an important factor of which is shared language). Thus, the greatest threat to societal security is the conversion of identity, when "people start to think of themselves as something else" – and at this point the issue is often transferred to the political sector. The role of the media, especially of news stories, is the presentation of events in terms of "us" and "them"[3]. Alien narratives provide an opposite perspective and interpretation, consequently, pose a threat to the cohesion and identity of the society.

If the issue is moved to the political sector, it is addressed as a political threat. On one hand, it may impact the ideology or other constitutive idea of the identity of a group or of a state and thus threaten internal legitimacy. On the other hand, an opposing strategic narrative may affect the external recognition of a group or of a state and thus threaten external legitimacy. This means that the sovereignty of a state or the legitimacy of a group can be contested from outside when its pillar, that is, its constitutive ideology is attacked.

The security problems of the modern media landscape

It is known that the sectors of security overlap and are not possible to clearly delineate. Media corporations, however, belong to more than one sector of security, similarly to other phenomena. Apart from their social role, they are profit-centred business enterprises, which hides their possible connections with states, usually, their home state. Consequently, the leading media corporations serve as effective tools of the projection of certain strategic narratives. The sale of news as a product is facilitated by a marketing strategy which emphasizes balance and objectivity, also promoting the ability of the media corporation to project specific strategic narratives[4]. The interpretive role of journalists in compiling facts and assembling them into "stories" or "plots" is quite evident. But the fragmentation of both the production and projection processes leads to the impression that the outside world is anarchic and impossible to understand. It also conceals the goal and lets news consumers focus on the minor goals only.

The products of the news industry coming from the international sphere, especially from the developed world influence home audiences in less developed countries more than the news flow from home sources.

---

[1] Council of the EU, *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU.* 2 https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/ (12.12.2024)

[2] Barry Buzan, Ole Waever, Jaap de Wilde, *Security: A New Framework for Analysis,* Lynne Rienner Publishers Inc., Boulder, Co., 1998, pp. 119-140

[3] *Idem*, pp. 122-124

[4] Clausen, Lisbeth, *International News Flow*, in Allen Stuart (Ed.), *The Routledge Companion to News and Journalism,* Routledge, Taylor and Francis Group, London and New York, 2010, p. 131

Thus, the international news industry reinforces the values of capitalism and the strategic narratives of the elites of leading industrialised states. The concentration of media content production poses a risk to the plurality of opinions and to societal security.

According to Google, currently the most important news agencies in the world are as summarised in Table 1. Seven out of the 18 agencies in the rank are from English speaking countries, which reflects the dominance of their language and their news storytelling. Another five can be added representing Western values from France, Spain, Italy, Germany and Japan. Beside the mentioned twelve agencies, those of regional powers are included from Turkey, India and Egypt. The greatest rivals of the Western worldview and strategic narrative, Russia and China are represented by one news agency each: TASS and Xinhua.

Name of news agency	Country of origin
Agence France-Presse	France
Agencia EFE	Spain
Agenzia Nazionale Stampa Associata	Italy
Anadolu Agency	Turkey
Asian News International	India
Associated Press	USA
BBC Scotland	UK
Bloomberg	USA
Deutsche Presse-Agentur	Germany
Kyodo News	Japan
Middle East News Agency	Egypt
Press Trust of India	India
Reuters	UK
TASS	Russia
The New York Times	USA
The Washington Post	USA
United Press International	USA
Xinhua	China

Table 1. Leading news agencies of the world[1]

It seems that, below the surface of institutionalised news production and recognised news agencies, that is, the so-called conventional media, contestation and persuasion are ongoing in the social media. One reason can be its "grey zone" character: the lack of legal regulation, the difficulty of identification of sources and actors, and the lack of technological knowledge of the users, which grants almost unlimited power to the platform operators over the consumers[2]. When social media was a novelty, consumers believed it the most democratic forum for communication in society because most of its content would be user created. Instead, user generated content, including clicked-on websites and recording the length of time spent viewing them

[1] Author's compilation based on Google

[2] Søren Vigild Poulsen, Gunhild Kvåle, *Studying social media as semiotic technology: a social semiotic multimodal framework*, "Social Semiotics", Vol. 28 No. 5, 2018, pp. 700-717, https://doi.org/10.1080/10350330.2018.1505689 (21.11.2024)

were monitored by the platform operators, justified by commercial and marketing purposes. Soon the method was transferred to political marketing activities, and now both the methodology and much of the technology (data mining software's, bots and botnets) are available to anyone.

User profiling, as it was said above, allows data collection on personal qualities of digital media users, probably violating their privacy. It is not known how the data are collected, where the data are stored and processed. Figure 1 proves the detailed profiling of US citizens for the 2024 election campaign. The same is probably true for any state's citizens nowadays if they use digital devices.

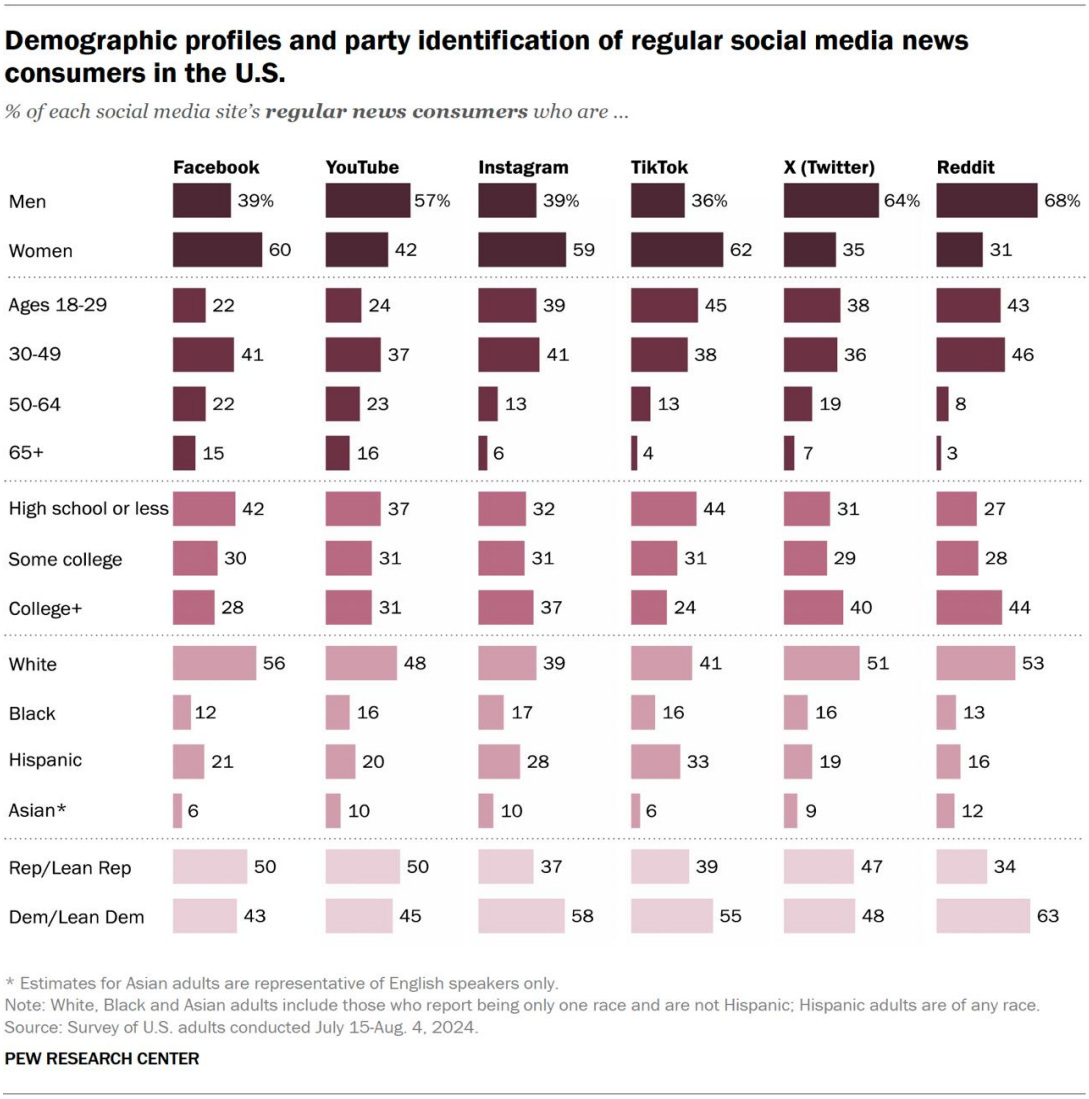

Figure 1. An example for user profiling: The demographic profiles of social media consumers in the US in 2024[1]

If giant tech corporations have opportunity to collect data on the society of any state, it may pose a security risk, especially if they, as it is experienced nowadays, create their own regulations which affect not only consumer behaviour but also freedom of speech. Apart from the regulations, technological solutions can influence the visibility and accessibility of posts and commercials. But the most dangerous interference in a society's life is probably falsifying societal preferences by using bots and botnets to boost shares, likes and dislikes. This may threaten societal security because it fakes majority and thus "hijacks" democratic will. It results in confusion and disturbances and shatters the citizens' trust in democratic institutions.

[1] https://www.pewresearch.org/journalism/2024/09/17/appendix-demographics-and-party-identification-of-regular-social-media-news-consumers-in-the-united-states/ (21.11.2024)

Although conventional media is still popular among news consumers, social media sources gain more and more ground. This highlights why the merge of genres, professional journalism and private communication endanger security: news consumers can be exposed to alien strategic narratives unnoticed. Nevertheless, the securitisation of media ownership and media control, apart from the usual antitrust regulations, is inconceivable because of the values of Western democracies and because profits, competition and discourse about fast technological development legitimise grey zone for the media platforms.

Securitization in wartime: a case study

As it was mentioned above, the EU-imposed ban on two Russian media outlets, Russia Today and Sputnik in 2022, is a recent example of securitization of media. Council Regulation (EU) 2022/350 of 1st of March 2022[1] reflects that the securitization of the mentioned media outlets was a long process: the council decision amended Regulation (EU) No 833/2014[2] created in response to the Russian annexation of the Crimea, which did not yet affect the Russian media broadcast in the EU. The mentioned 2022 Regulation states that the two media outlets "are engaged in propaganda actions." The following paragraph illustrates how rival strategic narrative works and which aspects of society it targets: "(6) The Russian Federation has engaged in a systematic, international campaign of media manipulation and distortion of facts to enhance its strategy of destabilisation of its neighbouring countries and of the Union and its Member States. In particular, the propaganda has repeatedly and consistently targeted European political parties, especially during election periods, as well as targeting civil society, asylum seekers, Russian ethnic minorities, gender minorities, and the functioning of democratic institutions in the Union and its Member States". The paragraph below hints at the dissemination of the Russian strategic narrative by the mentioned and other media outlets.

It also proves that technology allows a proliferation of sources, which makes the spread of unreliable or false information uncontrollable: "(8) Those propaganda actions have been channelled through several media outlets under the permanent direct or indirect control of the leadership of the Russian Federation. Such actions constitute a significant and direct threat to the Union's public order and security". The regulation also cites Article 11 of the Charter of Fundamental Rights[3], which says "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety**,** for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". (Emphasis by the author.)

The emphasis we added in italics underscores that the Charter of Fundamental Rights allows certain procedures for maintaining national security, territorial integrity and public safety. Besides, it places these procedures in the context of states, consequently, recognises the right of a state to securitize media if deemed necessary. Regarding the interrelationships between societal security discussed above and national security, the latter can be interpreted as the protection of the components of the state from outside threats and interference according to Buzan[4]. What prevents the full securitization procedure by the EU is hinted at by mentioning

[1] *Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.065.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A065%3ATOC (21.11.2024)

[2] *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0833 (21.11.2024)

[3] *EU Charter of Fundamental Rights,* Article 11, https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information (21.11.2024)

[4] Barry Buzan, Ole Waever, Jaap de Wilde, *Op. cit.*, 100

Article 16 titled Freedom to conduct a business[1] and Article 17 on Right to property[2]. This sheds light on the reason for avoiding securitisation of the media: it would be contrary to some civil liberties as well as the freedom of enterprise in capitalism. Thus, the regulation mitigates the impact of the suspension of broadcast license (not a final prohibition) and its consequences: "(11) Consistent with the fundamental rights and freedoms recognised in the Charter of Fundamental Rights, in particular with the right to freedom of expression and information, the freedom to conduct a business and the right to property as recognised in Articles 11, 16 and 17 thereof, these measures do not prevent those media outlets and their staff from carrying out other activities in the Union than broadcasting, such as research and interviews". The EU is in a trap concerning media securitisation because this would be against the Union's fundamental principles. One of the outcomes of the efforts to try to follow advancements in digital technology and the proliferation of platforms and regulate online content and services in the interest of EU citizens may have been the Digital Services Act (DSA) approved by the Council of the European Union on 4 October 2022 and enacted on 17 February 2024[3].

The case of Russia Today and Sputnik can be examined from the aspect of the components of securitization to draw consequences. Buzan et al.[4] include three units in their securitization theory, underlining that the procedure is more important than the exact constituents: the referent object, the securitizing actor and the functional actor. The referent object is a thing that is existentially threatened although it has legitimate claim to survival. The securitizing actor is someone or something that declares that the referent object is existentially threatened. The functional actor is the one that influences the dynamics of securitization without being a referent object or a securitizing actor. Generally, thinking within the conventional framework of a state, the referent object is either the state or the nation; the securitizing actor is a government or a political personality, and the functional actor could be, for instance, an enemy state, a terrorist organisation or an industrial corporation.

Who is who in the case described above? Buzan et al. remark that sets of rules or principles may also become referent objects in the securitization process: for example, "liberal world economy" and "free trade"[5]. In the case of the sanctions imposed on Russian media outlets, the referent objects are the values included in the Charter of Fundamental Rights discussed above. The securitizing actor is the European Union. The functional actor is the Russian media outlets or, indirectly, the leadership of the Russian Federation. Nevertheless, what would an existential threat mean in the case of European values is difficult to interpret, since, as it was pointed out above, the media belongs to at least three sectors of security: political, economic and societal. The economic sector was de-securitized after the Second World War because of gradual economic liberalization. Political security involves the organizational stability of social order as well as the sovereignty of a state. The quotes from Council Regulation (EU) 2022/350 imply that, in the narrow sense, societal security is the referent object of securitization.

To sum up, societal security and political security are interrelated and overlap, while economic security seems to be easier to delineate. The problem with securitization of the media in the case discussed is that, focusing on political security, stability and/or sovereignty could be the referent object, while, by shifting the focus on societal security, social peace and/or identity could be the referent object. However, both are difficult to imagine outside the context of the state, within the framework of the EU, because the EU is not a state (though it has some state-like features) and does not have sovereignty, what is more, researchers disagree over the existence of European identity. The concept of society is also hard to apply generally in the EU context because its member states do not have uniform societies. In addition, the securitization of the two Russian media outlets contradicts the principles of liberal economy, which belong to the fundamental ones of the EU.

---

[1] *EU Charter of Fundamental Rights Article 16*, https://fra.europa.eu/en/eu-charter/article/16-freedom-conduct-business (21.11.2024)

[2] *EU Charter of Fundamental Rights Article 17*, https://fra.europa.eu/en/eu-charter/searchresults?combine=Article+17 (21.11.2024)

[3] *The Digital Services Act (DSA)*, https://www.eu-digital-services-act.com/ (21.11.2024)

[4] Buzan, Barry; Waever, Ole and Wilde, Jaap de, *Security: A New Framework for Analysis.* Lynne Rienner Publishers Inc., Boulder, Co., 1998, p. 36

[5] *Ibidem*, p. 38

On 30 May 2024, an article was published on the home page of the New York Times claiming that, according to a study, hundreds of websites were multiplying and disseminating Russia Today produced content in EU member states.[1] The study proved that unsuspecting internet users were exposed to RT propaganda on seemingly innocent, family issues related websites. The journalists sent an email inquiring who operated the website and where it was registered but received no answer. This is evidence of the ease with which modern technology allows the circumvention of any legal regulation. The legal aspects of the case were discussed in European Papers[2].

Conclusions

The article has tried to analyse the interconnections between technological advancements and the dissemination of strategic narratives, assessing the possibly resulting security risks for societal security. The sectoral theory of the Copenhagen School was used as theoretical background and securitization theory was used as methodological framework for analysis. I have summarised the still prevalent effect of the work of conventional news agencies, which spread news stories developed mostly with Western perspective; however, news agencies of rival powers are also active and on the rise.

Research question 1 asked "What changes have occurred in the production of strategic narratives in the digital era?" I have found that digital technology has caused profound changes in the formation, projection and reception of strategic narrative. One remarkable result is the adaptability of its formation because data collection on users allows more purposeful design and flexible and fast response. This major change has led to an erosion of legal regulations which are not always applicable to new technological advancements and the resulting alterations in journalistic work methods and professional standards. In fact, the boundary between professional journalism and social media users' texts seems to be blurring. It leads to a simplification of messages in strategic narratives as well as a shift of focus from verbal texts to visual texts, especially photos and videos, which are technologically easy to falsify and more difficult to trace back to their source. In addition, human language has been used for millenniums, thus, verbal signs of lying are more commonly recognised than deception achieved with innovative technological tricks. The short and simplified stories break up the strategic narrative and better hide its goal, that is, persuasion in an actor's interest. Due to user profiling and other ways of data mining, the projection of strategic narratives has become more targeted and more efficient.

Research question 2 was "How does the interference of opposing strategic narratives impact societal security?" I have summarised the concept of societal security and highlighted that strategic narrative creates the cohesion in society which provides societal security. If the strategic narrative of a community is broken up or challenged, for instance, because adversarial narrative is mixed into it and this fact remains unnoticed by the population, it can be considered a threat to societal security. If the rival strategic narrative is efficient, it may lead to questioning the legitimacy of the social order and the political system, thus, posing a threat to the sovereignty of a state. The latter is especially true because, on social media, either a disruptive internal group or an external power may create an impression of majority with technological tricks. The dangerous innovation is, that earlier the enemies tried to influence mostly the decision-makers and the external source of this attempt could be detected. Because of the opportunities of digital technology, now external influence on the decision-makers can be disguised as internal, that is, as if it represented the public opinion of their own society.

The case study has proven that digital technology mediated adversarial strategic narratives threaten societal security because they attack Western democratic values by abusing these values. For example, since stricter regulation of the media would impact basic democratic freedoms like freedom of speech, of expression, of the media, among others. What is more, news reporting and media are cross-sectoral, that is, they are interconnected with more than one sector of security: societal, political, economic, and even the military sector. Although we have seen examples when certain news media were suspended or banned in a country or an international organisation because of an armed conflict or war, still, the Western values, the political interests of status quo states and economic interest of giant media corporations currently prevent such a move.

[1] https://www.nytimes.com/2024/05/30/business/media/russia-rt-disinformation-europe-ban.html (21.11.2024)

[2] Ferenc Gergely Lendvai, *Media in War: An Overview of the European Restrictions on Russian Media*, "European Papers", 2023, Vol. 8, No. 3, pp. 1235-1245, https://www.europeanpapers.eu/es/europeanforum/media-in-war-overview-of-european-restrictions-on-russian-media (21.11.2024)

In summary, hybrid warfare is continuing in all fields of life, from economy through politics to military conflicts. The same process is reflected by the contestation of strategic narratives in the digital media. Whose story wins in the global power shift is to a large extent dependent on the construction of new strategic narratives and the strategic use of the digital media.

Bibliography

Books

1. Allan, Stuart (Ed.), *The Routledge Companion to News and Journalism*, Routledge, Taylor and Francis Group, London and New York, 2010
2. Buzan, Barry, *People, States, and Fear. An Agenda for International Security in the Post-Cold War Era.* Lynne Rienner Publishers Inc., Boulder, Co., 1991
3. Buzan, Barry; Waever, Ole; Wilde, Jaap de, *Security: A New Framework for Analysis.* Lynne Rienner Publishers Inc., Boulder, Co., 1998
4. Jowett, Garth S.; O'Donnell, Victoria J., *Propaganda and Persuasion*, SAGE Publications, 2015
5. Miskimmon, Alister; O'Loughlin, Ben; Roselle, Laura, *Forging the World: Strategic Narratives and International Relations*, University of Michigan Press, 2017
6. Nye, Joseph S., *Soft Power: The Means to Success in World Politics*, Public Affairs, New York, 2004
7. Taylor, Bryan. C.; Bean, Hamilton. (Eds.), *The Handbook of Communication and Security*, Routledge, Taylor and Francis Group, New York, London, 2019

Studies and Articles

1. Antoniades, Andreas; Miskimmon, Alister; O'Loughlin, Ben, *Gr5,* https://www.sussex.ac.uk/webteam/gateway/file.php?name=cgpe-wp07-antoniades-miskimmon-oloughlin.pdf&site=359ps://www.sussex.ac.uk/webteam/gateway/file.php?name=cgpe-wp07-antoniades-miskimmon-oloughlin.pdf&site=359
2. Bakir, Vian; Herring, Eric; Miller, David; Piers, Robinson, *Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture*, "Critical Sociology", Vol. 45, No. 3, 2018, DOI: 10.1177/0896920518764586
3. Cull, Nicholas J., *Public Diplomacy: Taxonomies and Histories*, "The Annals of the American Academy of Political and Social Science", Vol. 616, Public Diplomacy in a Changing World, March 2008
4. Fink, Udo; Gillich, Inez, *Fake News as a Challenge for Journalistic Standards in Modern Democracy*, "University of Louisville Law Review", Vol. 58, Issue 2, Spring 2020
5. Lendvai, Ferenc Gergely, *Media in War: An Overview of the European Restrictions on Russian Media*, "European Papers," Vol. 8, No. 3, 2023, https://www.europeanpapers.eu/es/europeanforum/media-in-war-overview-of-european-restrictions-on-russian-media
6. Poulsen, Søren, Vigild; Kvåle, Gunhild, *Studying social media as semiotic technology: a social semiotic multimodal framework*, "Social Semiotics", 28(5), 2018, https://doi.org/10.1080/10350330.2018.1505689
7. Price, Monroe, E.; Haas, Susan; Margolin, Drew, *New Technologies and International Broadcasting: Reflections on Adaptations and Transformations*, "The Annals of the American Academy of Political and Social Science", Vol. 616, Public Diplomacy in a Changing World, March 2008

Documents

1. Council of the EU, *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*, 2 March 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/
2. *EU Charter of Fundamental Rights Article 11,* https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information
3. *EU Charter of Fundamental Rights Article 16,* https://fra.europa.eu/en/eu-charter/article/16-freedom-conduct-business
4. *EU Charter of Fundamental Rights Article 17,* https://fra.europa.eu/en/eu-charter/searchresults?combine=Article+17

5. *The Digital Services Act (DSA)*, https://www.eu-digital-services-act.com/
6. *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0833
7. *Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.065.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A065%3ATOC

Internet sources

1. https://eur-lex.europa.eu/
2. https://fra.europa.eu/
3. https://www.consilium.europa.eu/
4. https://www.eu-digital-services-act.com/
5. https://www.europeanpapers.eu/
6. https://www.europeanpapers.eu/
7. https://www.nytimes.com/
8. https://www.pewresearch.org/
9. https://www.sussex.ac.uk/

Dorel DANCIU
Babeș-Bolyai University of Cluj-Napoca, Romania

SOCIAL MEDIA AND THE FIGHT FOR HEARTS AND MINDS: GENERATIVE ARTIFICIAL INTELLIGENCE AS POLITICAL CAMPAIGN INFLUENCE TOOL

Abstract:	*Social networks are important tools at the hands of political actors due to the direct connection with voters. Candidates and campaign teams can easily send messages to voters and can also see how they react to those messages and access the personal data available in each account. From the aggregation of this data through specific technical instruments, it is also possible to obtain segmented voting profiles. Campaign teams can thus adapt their communication flow to the expectations of the electorate and develop campaign strategies based on data.* *In the era of digital revolution, political actors' use of generative artificial intelligence through social media gives them the ability to create personalized messages, but also to accurately estimate their impact on individuals and groups. Different state and non-state entities can interfere with ongoing campaigns, influencing the electorate by favoring certain political actors and jeopardizing the democratic practices that should govern the electoral process.*
Keywords:	**Social media; political communication; generative AI; influence; disinformation; online propaganda**
Contact details of the authors:	E-mail: dorel.danciu@ubbcluj.ro
Institutional affiliation of the authors:	**Doctoral School of Sociology, Babeș-Bolyai University of Cluj Napoca, Romania**
Institutions address:	21Dec.1989 Bd.,128, Cluj-Napoca, 400604, 0040.264419958, socasis.ubbcluj.ro, secretariat.socasis@ubbcluj.ro

Introduction

In the era of the digital revolution, social networks have become very effective tools in communicating messages from political actors to voters, influencing personal beliefs, shaping public opinion and, finally, determining voter behavior. Platforms like Facebook, X (former Twitter), Instagram and TikTok serve not only as channels of communication, but also powerful tools of influence and persuasion. This paper explores the mechanisms of influence and persuasion in social media, examining how these platforms work, the methods used by influencers and politicians, and the implications for electoral process in the times of generative AI (GenAI). The presentation of the theoretical concepts will be followed by practical examples, to reinforce the theoretical approach.

Social media influence, persuasion and propaganda

"Social Influence Theory", originally formulated by Herbert Kelman in 1953 is the starting point in explaining conditions under which social influence determines a change in attitude or behavior and highlights the fact that there are three modes of social influence acceptance: namely compliance, identification, and internalization[1]. Social media influences political opinions through various mechanisms including social proof, emotional appeals, and the influence of influencers, which are among Robert Cialdini's principles of influence[2]:

[1] Dinara Davlembayeva, Savvas Papagiannidis, *Social Theory: A Review*, in Savvas Papagiannidis (Ed.), *TheoryHub Book*, 2024, https://open.ncl.ac.uk/theory-library/social-influence-theory.pdf (05.11.2024)

[2] Robert Cialdini, *Psihologia persuasiunii: totul despre influențare*, Bussiness Tech International, București, 2014, pp. 11-15

(1) Social proof: The concept of social proof suggests that individuals are influenced by the actions and opinions of others. Social proof is the tendency to believe something not because there are good arguments but because a lot of others seem to believe it[1]. On social media, users often align their beliefs with those prominently displayed by their peers, public figures, or trending topics.

(2) *Emotional engagement***:** Emotion plays a critical role in persuasion and tailor to a cognitive vulnerability[2]. Social media allows for the rapid dissemination of emotionally charged content, such as videos, memes, and stories that evoke feelings of hope, fear, or outrage.

(3) *Influencer Endorsements:* The rise of social media influencers has introduced a new layer of persuasion in political campaigns. Influencers, who wield significant reach and credibility among their followers, can sway public opinion when they endorse candidates or issues.

Among the many models of influence of mass communication, the one developed by Elizu Katz and Paul F. Lazarfeld in 1955, adapted to the reality of the digital revolution we are experiencing, retains its relevance. The *two-step flow of communication* model was developed following research conducted during the 1940 United States presidential election campaign and concluded that mass media operate in a very complex network of social relationships, and the number of those who receive the media message (individuals) is higher than those who are directly exposed to the message (opinion leaders)[3]. According to this model of interpersonal influence, the effects of exposure to messages are not felt immediately, they are determined by the multitude of social relationships created around opinion leaders. There are two processes, one of receiving the message, the other of accepting or rejecting the message sent to influence. Opinion leaders are the most active within social networks and are responsible for receiving, processing influence and transmitting the message coming from the media to other members of the social network.

Closer to the present day, Duncan Watts and Peter Dodds in 2007 adapted the model by insisting that opinion leaders are not leaders in the true sense of the word and that they act as intermediaries between the media and the public, called *influencers* or *stars*. They are trusted advisors who try to produce interpersonal changes on *followers* to create a desirable public opinion[4]. In 2022, Seth Kline, Jonathan Ritschel and Robert Fass renamed the term influencer with star, recognizing the effect of *stars* on society is amplified through social media.

This model of influence seems to be very well valued by social networks sites as intermediaries and message amplifiers between influencers and non-influencers[5]. Nowadays, part of the role of mass media as an intermediary between opinion leaders and the public has been taken over by social networks such as Facebook, Instagram, X, and You Tube.

[1]James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed, *Countering Information Influence Activities*, https://rib.msb.se/filer/pdf/28697.pdf, p. 36 (25.10.2024)

[2]*Ibidem*, p.63

[3]Denis McQuail, Sven Windahl, *Modele ale comunicării pentru studiul comunicării de masă*, Comunicare.ro, București, 2004, pp. 55-57

[4]Duncan J. Watts, Peter Sheridan Dodds, *Influentials, Networks, and Public Opinion Formation*, "Journal of Consumer Research", Vol. 34, No. 4, 2007, pp. 441-443

[5] Seth A. Kline, Jonathan D. Ritschel, Robert D. Fass, *Social Media, Public Opinion, and Resource Implications for the United States Air Force*,"Journal of Defense Resources Management", Vol.13, No. 2, 2022, pp. 35-37

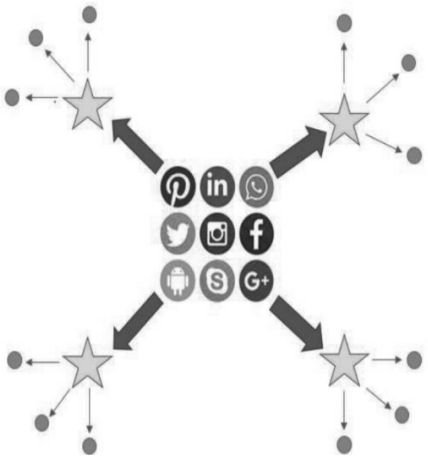

Fig. 1 The Star Model of Influence[1]

To illustraisthis model of influence with a practical example, we will present a short case study having as its subject the way in which the key messages of Russian propaganda are transmitted on the political scene in Romania by influential leaders. The results of an INSCOP survey, conducted in March 2024, show that Romanians consider social networks as the second main source of information (28.3%), after television (51.6%). The same sample surveyed believes that social networks are the main source of transmission of fake news and disinformation, with a percentage of 43%. In the opinion of 45.6% of Romanians, Russia is the main source of propaganda actions, disinformation and fake news in Romania. The percentage is significantly higher than that registered in January 2022, before Russia's armed aggression against Ukraine, when 27.3% believed that Russia supports propaganda actions, misinforms and spreads fake news in Romania. It should be noted that Romanians considered Russian propaganda as the main source of disinformation, even before the invasion of Ukraine[2].

Due to negative experiences in the common history, more recent or more distant (the end of WW II, the invasion of Czechoslovakia, the interference in the Transnistrian conflict), Romanians are not receptive to the messages directly transmitted by pro-Kremlin propaganda through assumed social media channels. This is the main reason why Russian disinformation is propagated through image vectors or influencers who amplify the message created most of the time outside the country's borders. Russian propaganda in Romania follows a regional trend, with the center of gravity on Ukraine and points of interest for the neighboring countries, especially the Republic of Moldova.

Russia's strategic objectives in Romania are to increase distrust within society, between society and government, and between Romania and its allies. This would make Romania a less reliable member of NATO and the European Union, undermining the Romanians' trust in democracy, liberal values, external alliances, thus promoting the destabilization and weakening of the country[3]. The Russian narratives are promoted in Romania by to types of political actors: (1) image vectors who assume the role of promoters of the Kremlin's messages, such as Diana Iovanovici Șoșoacă, the leader of the SOS party, who recently entered the European Parliament, and (2) politicians who do not recognize their affiliation with the pro-Kremlin propaganda, but through the messages sent in the public space they align perfectly with this propaganda, and this category generally includes the representatives of the AUR party and FIDESZ party with a significant influence among the Hungarian minority in Transylvania. The political message is also amplified by the journalists grouped in the new Press Club, founded in 2023.

---

[1] *Idem*

[2]INSCOP Research, *Disinformation, fake news, trust in information sources,* https://www.inscop.ro/martie-2024-sondaj-de-opinie-inscop-research-realizat-la-comanda-news-ro-partea-a-viii-a-dezinformare-stiri-false-increderea-in-surse-de-informatii/ (15.10.2024)

[3]Global Focus, *Foreign Information Manipulation and Interference Threats and Answers in Romania in the context of the war in Ukraine*, https://www.global-focus.eu/2024/10/foreign-information-manipulation-and-interference-threats-and-answers-in-romania-in-the-context-of-the-war-in-ukraine/ (30.10.2024)

In the context of the war in Ukraine, the main narratives[1] are generally anti-Ukrainian, anti-UE, and anti-NATO, rather than pro-Russian:

- Russia was forced to invade Ukraine as a result of the provocative actions of NATO, the EU and Ukraine;
- Ukraine has historical territorial disputes with Romania and ethnic Romanians in Ukraine are discriminated on the basis of language, religion and access to education in their mother tongue;
- EU/NATO protection against Russia's provocative actions is weak, and countries like Romania lack security guarantees in the event of an expansion of the war;
- The EU encourages the consumption of cricket flour, gives too many rights to sexual minorities and the environmental agenda affects the economic interests of citizens;
- Inflation and economic instability as a result of the armed conflict in Ukraine.

According to Expert Forum report[2], the Tik Tok network is the most used in terms of transmitting pro-Kremlin messages, and with the help of the Exolyt tool, anti-NATO propaganda videos were identified with over a million views in Romania, over 2200 of anti-EU videos and 1076 videos containing themes of territorial revisionism.

Disinformation and manipulation in online political campaigns

Social media provides suitable platforms for influence and persuasion but raises concerns about information authenticity and manipulation of voters. The rapid spread of misinformation poses significant challenges, as false narratives can quickly gain credibility through social sharing. This phenomenon has been particularly evident during political campaigns and COVID public health crises, where misinformation can lead to widespread confusion and potentially harmful behaviors.

In a general sense, *disinformation* represents the creation and distribution of false or misleading messages, with the aim of misleading the public and creating the desired effect on it[3]. While *misinformation* is an unintentional disinformation that consists in the transmission in the public space of information without real support without the obvious aim of causing damage to the public image, *malinformation* involves the intentional dissemination of content with the aim of producing negative effects on the intended target[4].

Social networks have amplified the importance of *fake news*, which are the basis of disinformation, misinformation and malinformation; fake news is news that claim to be factual, but which contain intentionally wrong information from a factual point of view, made with the intention of attracting the audience and deceiving[5]. Fact-checking is the process by which the accuracy of a news story is verified, in the effort to combat disinformation, before or after dissemination[6].

Along with disinformation, propaganda is another 'dark side' of online communication. According to H.D. Lasswell *propaganda* refers to the control of opinion by significant symbols, or to speak more concretely and less accurately, by stories, rumors, reports, pictures, and other forms of social communication. Propaganda is concerned with management of opinions and attitudes by the direct manipulation of social suggestion rather than by altering other conditions in the environment or in the organism[7].

---

[1] Global Focus Report, *Foreign Information Manipulation and Interference Threats and Answers in Romania in the context of the war in Ukraine*, https://www.global-focus.eu/2024/10/foreign-information-manipulation-and-interference-threats-and-answers-in-romania-in-the-context-of-the-war-in-ukraine/ (30.10.2024)

[2]Expert Forum, *Monitoring report -Architecture of Disinformation: Kremlin propaganda. Disinformation*, https://expertforum.ro/en/files/2024/09/Arhitectura-dezinformarii-romanesti-Relatia-cu-Kremlinul.docx-1.pdf-1.pdf-en.pdf (30.10.2024)

[3]European Commission, *Tackling online disinformation: a European Approach*, https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach (30.10.2024)

[4] Autoritatea Electorală Permanentă, *Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor*, https://www.roaep.ro/prezentare/wp-content/uploads/2024/03/GHID_GLFN_FINAL.pdf (25.10.2024)

[5] Bogdan Oprea, *Fake News și dezinformare online: recunoaște și verifică,* Polirom, Iași, 2021, p. 88

[6] *Ibidem*, p. 194

[7] Corneliu Bjola, *Propaganda as Reflexive Control. The Digital Dimension*.Countering *Online Propaganda and Extremism*, Routledge, 2018, p.14

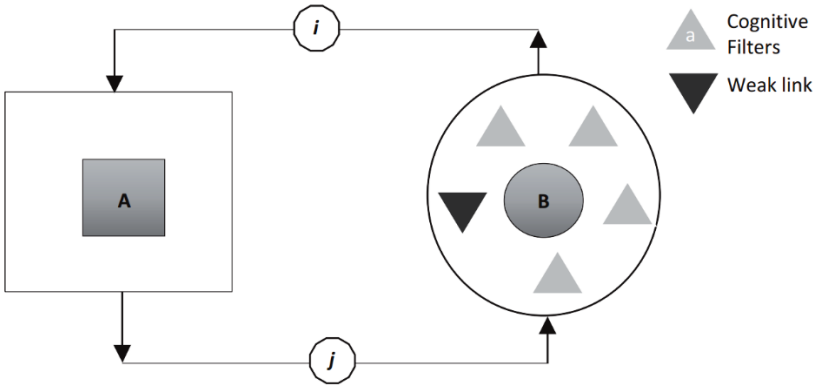

Fig. 2 Model of Reflexive Control[1]

In short, the *model of reflexive* control shows how propaganda campaigns work by suggesting that "gaining access to the cognitive filter by which an opponent makes sense of the world, the controling party might be able to induce him/her to voluntarily take decisions in favour or at least not against its interest"[2]. Fom the perspective of social media use, the data generated online are used to realize cognitive profiles of individuals using 4 layers of cognitive filters: conversation filter, network filter, demographic, and psychographic filter. Corneliu Bjola highlights five counter-disinformation tactics:

- Ignoring - official comunication flow will keep the discution focused on key message and prevent unnecessary escalation;
- Debunking - correct false and misleading statements by using factual evidence;
- Turning the tables - 'jiu-jitsu' principle of turning the opponent's strengths into a weakness;
- Discrediting the opponent - pro-active counter measure that consist of discrediting the opponent not to try undermine the credibility of the message;
- Disrupting - consist of disrupting the network the opponent uses for diseminating information online[3].

The following practical example wants to show how disinformation wears the latest techniques, which combine the use of social media, online news platforms and GenAI. In the last decade, the Republic of Moldova, like Ukraine, has been a kind of testing and training ground for Russian propaganda and its disinformation capabilities. Using key-message, thematic and similar methods, the pro-Kremlin propaganda tried by all possible methods to divert Moldova from the European path, to divide society, which is already fragmented from an ethnic point of view, and to make citizens to be less supportive to the process of integration into European institutions.

Disinformation actions reached their peak during the presidential elections in October this year, and the favorite target was the pro-European candidate, Maia Sandu. According to the European monitoring portal EUvsDisinfo, in the period before and after the elections there were no less than seven actions of transmitting fake news related to Maia Sandu and a possible fraud of the electoral process and the referendum.

Just two days before the voting day, to influence the outcome of the election, one of the Telegram propaganda channels transmitted false information according to which Maia Sandu suffered from schizophrenia and panic attacks, receiving treatment at a clinic in Vienna[4]. In support of this fake news, a medical document issued by a doctor of the clinic, most likely generated by AI, was posted. This fake news

[1] *Ibidem*, p.18
[2] *Ibidem*, p.17
[3] Corneliu Bjola, *The 'dark side' of digital diplomacy: countering disinformation and propaganda*, Routledge, https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari5-2019-bjola-dark-side-digital-diplomacy-countering-disinformation-propaganda.pdf, 2019 (20.10.2024)
[4] EUvsDisinfo, *Documents show Moldovan President Maia Sandu has schizophrenia* https://euvsdisinfo.eu/report/documents-show-moldovan-president-maia-sandu-has-schizophrenia/ (20.10.2024)

was automatically picked up by a Pravda page, in Spanish and English, to engage the press on a much higher level.

Generative AI as political campaign influence tool

Generative AI (GenAI) is an advanced type of machine learning that comes with a new and advanced tool based on technology mainly intended for creating, disseminating text, image and video messages of political actors and analyzing the effects on the target audience[1]. Initially used in marketing and fundraising campaigns, generative AI can fundamentally change the way electoral campaigns are conducted. Based on Large Language Models (LLMs) and Large Visual Models (LVMs) generative AI has the possibility of analyzing very large amounts of data, from the perspective of opinions, online behavior, areas of interest of individuals who are under various digital identities. These individuals, potential voters, are grouped by category according to their opinions and common interest, in the process of segmenting the target audience. The next stage of the process is the elaboration of messages adjusted to the previously identified audience categories. This cyclical process can be supplemented with a further evaluation of the effect on the voters in terms of change in perception, opinions or behavior because of exposure to the messages. Based on *Large Language Models* (LLMs) and *Large Visual Models* (LVMs), GenAI could accomplish the main following tasks[2]:

· Generate image, audio and video and detection of AI generated image, audio and video content;

· Generate text end detect the AI generated text.

As a *microtargeting* tool[3], GenAI can conduct data analysis and insights processing large volume of social media data (text, video, audio, image) and extract important identify trends, key influencers, perspectives on a fact, the main concerns of the public based on:

· Social listening and monitoring - through algorithm-based tools, GenAI can monitor social media in real time by identifying brand mentions, customer feedback and emerging trends. From this process can result an almost exact perspective on the preferences of the target audience, the feeling towards an organization and the levels of involvement in supporting the politics of this organization.

· Social media influencer identification - based on conversational dynamics and reactions to messages, GenAI can contribute to the process of identifying relevant influences in a certain campaign.

· Voter's segmentation – GenAI can aggregate social media users based on their behavior and preferences. This helps political actors create personalized messages for different people audience segments achieving very good results in terms of attachment and a better understanding of specific political objectives.

Malicious use of microtargeting and GenAI is that it provides support for misinformation and disinformation activities, associated in most cases with political propaganda. The use of information and communication technology to monitor, coerce, deter, manipulate individuals or groups to discourage certain activities or beliefs is defined as *digital repression*[4]. Algorithms, automation, and AI are working together to improve efficiency, and sophistication of manipulation of public opinion online[5]. The most relevant examples of malicious use of GenAI, associated with disinformation and online propaganda, are AI generated text and audio, video, and image deepfakes[6]. *Deepfakes* are manipulated audio-visual material which is virtually

[1] William Marceliano, Nathan Beauchamp-Mustafaga, Amanda Kerigan, Lev Navare Chao, Jackson Smith, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0*, https://www.rand.org/pubs/perspectives/PEA2679-1.html (25.10.2024)

[2] Kalina Boncheva (Ed.), *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities*, https://edmo.eu/wp-content/uploads/2023/12/Generative-AI-and-Disinformation_-White-Paper-v8.pdf (25.10.2024)

[3]Sourav Majumdar, *Large Vision Models (LVMs): The next branch on the evolutionary tree and how it can help Marketers*, https://www.position2.com/blog/author/sourav-m/ (25.10.2024)

[4] Katarina Kertysova, *When 5G Meets AI: Next Generation of Communication and Information Sharing*, February 2022, https://stratcomcoe.org/publications/when-5g-meets-ai-next-generation-of-communication-and-information-sharing/237 (05.11.2024)

[5] *Idem*

[6] Kalina Boncheva (Ed.), *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities*, https://edmo.eu/wp-content/uploads/2023/12/Generative-AI-and-Disinformation_-White-Paper-v8.pdf (25.10.2024)

indistinguishable from real material[1]. GenAI can produce fully synthetic manipulated text, images, audio, and video, misleading voters and undermining governments' capacity to engage with citizens and influencing public opinion and deepening societal divisions.

Deceptive identities[2] are an umbrella that covers: (1) *shills* – dedicated manipulators that give the impression that are neutral; (2) *impersonators* - persons hiding behind another identity; (3) *impostors* – pretend to have skills that they don't possess; (4) *hijackers* – people who take over a social media account for the purpose of using it in their own interest. On the other hand, a *troll* is "a user of an online social platform who deliberately tries to aggravate, annoy, disrupt, attack, offend or cause trouble by posting provocative and unconstructive content"[3]. From a technical point of view, GenAI could clone existing social media accounts or create fake depersonalized accounts. *Bots* and *botnets* are pieces of automated computer software that performs tasks based on algorithms, and act as force multipliers for influence activities[4].

The following examples show how GenAI can decisively influence the outcome of the elections. According to political analysts, the results of the last legislative elections in Slovakia, organized in 2023, were decisively influenced by an election manipulation action that had as its point of origin pro-Kremlin propaganda. It was the first case in which an AI generated deepfake was able to decisively influence the outcome of an election. According to the publication *Wired*, two days before the date of the elections, a fake audio recording was intensively promoted through the Facebook network, which featured a dialogue between a well-known journalist and the leader of the main Slovak opposition party, Progressive Slovakia, Michal Simecka. He was making revelations related to a massive election fraud operation by buying votes from the Roma minority[5].

Later, conclusive evidence was brought forward that this case was an audio deepfake and that the audio recording was made with the help of Generative AI. This was also confirmed by the information verification department of the AFP news agency. The timing of the distribution of the recording was chosen in such a way as to cancel or limit the reaction of combating deepfake by the protagonists, due to the provisions of the electoral law of prohibiting advertising through the mass media 48 hours before the start of the poll. Instead, in the two days this recording was massively destroyed on social networks, including by opinion leaders. A contributing factor to the manipulation was that under Meta policies at the time, only deepfake video content could be criminalized. The main beneficiary of the manipulation was the Russia-sympathetic party that won the election, SMER, led by Robert Fico.

Conclusions

Social media are appropriate platforms for manipulation, misinformation and propaganda available to political actors. In this respect, media literacy programs for citizens are essential, to distinguish truth from falsehood. Well-coordinated strategic communication and transparency are very important for citizens to feel informed and valued, eliminating the desire to turn to populist and manipulative narratives.

In the usual way, through specific social media analytics and social media listening tools, public data can be extracted from individual accounts in social networks to create individual profiles, which include preferences and consumption habits. In the classical way, this process requires the use of specialized personnel and significant financial and time resources. The great advantage of using AI algorithms is a relatively low cost, the ability to use large amounts of data and the ability to disseminate messages to many recipients, having very good results especially in the activity of mobilizing voters and obtaining financial support for political campaigns. The flow of AI microtargeting can be summarized in the following steps: collecting data

[1] James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed, *Countering Information Influence Activities*, https://rib.msb.se/filer/pdf/28697.pdf, p.45 (25.10.2024)

[2] *Ibidem*, pp. 55-56

[3] James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed, *Countering Information Influence Activities*, https://rib.msb.se/filer/pdf/28697.pdf, p.62 (25.10.2024)

[4] *Ibidem*, pp. 56-59

[5] Morgan Meaker, *Slovakia's Election Deepfakes Show AI is a Danger to Democracy,* https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/ (25.10.2024)

from individual profiles, forming groups of people likely to react in the same way to identical messages, and sending messages tailored to previously identified groups.

The use of microtargeting and GenAI also raises serious legal and ethical issues and is in a gray area of political communication because of how voters' personal data is accessed. The use of microtargeting and generative AI also comes with a series of shortcomings or adverse effects. First, it raises serious questions about the use of personal data of social media users and the fact that they are processed without the consent of the owners. Even if these data are public, the purpose of their processing is different than the one for which these data are available.

Human-like behavior of GenAI systems are advancing day by day, increasing accuracy of malicious use such as deepfakes and generated text, and decrease confidence in electoral process and democracy. As a result, it is necessary to improve the ability of political campaign staff to detect AI generated content. It is necessary to regulate the use of AI in campaigns at de national level, in accordance with the EU AI Act and require labelling for some AI generated content.

Bibliography

Books

1. Bjola, Corneliu; Pamment, James, (Eds.), *Countering Online Propaganda and Extremism. The Dark Side of Digital Diplomacy*, Routledge, 2019
2. Boncheva, Kalina (Ed.), *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities*, "EDMO", 2024
3. Cialdini, Robert, *Psihologia persuasiunii: totul despre influențare*, Bussiness Tech International, 2014
4. Marceliano, Wiliam; Beauchamp-Mustafaga, Nathan; Kerigan, Amanda; Navare, Chao, Lev; Smith, Jackson, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0*, RAND Corporation, 2023
5. McQuail, Denis; Windahl, Sven, *Modele ale comunicării pentru studiul comunicării de masă*, Comunicare.ro, 2004
6. Pamment, James; Nothhaft, Howard; Agardh-Twetman, Henrik; Fjällhed, Alicia, *Countering Information Influence Activities*, Swedish Civil Contingencies Agency (MSB), 2018

Studies and Articles

1. Bjola, Corneliu, *The 'dark side' of digital diplomacy: countering disinformation and propaganda,* "ARI", No. 5, 2019
2. Davlembayeva, Dinara; Papagiannidis, Savvas, *Social Influence Theory: A review*, S. Papagiannidis (Ed.), "TheoryHub Book", 2024
3. Duncan, J., Watts; Dodds, P., Sheridan, *Influentials, Networks, and Public Opinion Formation*, "Journal of consumer research", Vol. 34, No. 4, 2007
4. Kertysova, Katarina, *When 5G Meets AI: Next Generation of Communication and Information Sharing*, February 2022, NATO STRATCOM COE, Riga
5. Kline, A. Seth; Ritschel, D., Jonathan; Fass, D., Robert, *Social Media, Public Opinion, and Resource Implications for the United States Air Force*, in Journal of Defense Resources Management, Vol. 13. No. 2, 2022

Press Articles

1. Meaker, Morgan, *Slovakia's Election Deepfakes Show AI Is a Danger to Democracy*, October 3, 2023, https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/
2. Majumdar, Sourav, *Large Vision Models (LVMs): The next branch on the evolutionary tree and how it can help Marketers*, https://www.position2.com/blog/author/sourav-m/

Documents

1. Autoritatea Electorală Permanentă, *Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor*, 2024
2. European Commission, *Tackling online disinformation: An European Approach*, Brussels, 26.4.2018, COM(2018) 236 final

3. Expert Forum, *Monitoring report - Architecture of Disinformation: Kremlin propaganda. Disinformation,* https://expertforum.ro/en/files/2024/09/Arhitectura-dezinformarii-romanesti-Relatia-cu-Kremlinul.docx-1.pdf-1.pdf-en.pdf
4. Global Focus, *Foreign Information Manipulation and Interference Threats and Answers in Romania in the context of the war in Ukraine*, September 2024
5. INSCOP Research, *Disinformation, fake news, trust in information sources*, March 2024, www.inscop.ro

Websites

1. https://euvsdisinfo.eu/
2. https://expertforum.ro/
3. https://www.global-focus.eu/
4. https://www.inscop.ro/en/home/
5. https://www.roaep.ro

Andreea Alexandra DINCĂ
Lucian Blaga University of Sibiu, Romania

ARTIFICIAL INTELLIGENCE IN THE EUROPEAN UNION. LEGISLATIVE BENEFITS AND CHALLENGES OF NON-COMPLIANCE

Abstract:	*The legislative benefits of artificial intelligence (AI) are multifaceted, driving innovation and economic growth while safeguarding citizens' rights. Clear regulations foster a trustworthy environment for investments, facilitating job creation and enhanced efficiency across various sectors, such as healthcare and education. For instance, AI can improve medical diagnostics through advanced data analysis, leading to the discovery of new treatments. The General Data Protection Regulation (GDPR) exemplifies the EU's commitment to protecting personal data, thereby boosting public trust in technology. Furthermore, legislation promotes ethical AI solutions, addressing social and moral implications to prevent abuses. Standardization and interoperability enhance international collaboration and efficiency among AI systems. However, non-compliance with these regulations poses significant risks, including security breaches, discrimination, and severe legal consequences. Organizations face substantial fines for violating laws like GDPR, which can reach up to 4% of global annual revenue. This uncertainty may hinder innovation and complicate international partnerships. Ultimately, while the European AI regulatory framework presents substantial opportunities for economic and social advancement, it is crucial that stakeholders adhere to these standards to ensure ethical and responsible use of AI, safeguarding fundamental rights and fostering sustainable development in society.*
Keywords:	**Artificial Intelligence; intelligence innovation; technology; big data; data protection; human rights**
Contact details of the authors:	E-mail: deea_18dei@yahoo.com
Institutional affiliation of the authors:	**Lucian Blaga University of Sibiu**
Institutions address:	10 Victoriei Blvd. Sibiu, code 550024, Phone: +40-(269) 21.81.65, Site: https://www.ulbsibiu.ro, E-mail: rectorat@ulbsibiu.ro

Introduction

Artificial Intelligence (AI) is transforming different sectors across the globe, including the European Union (EU) as the forefront of this technological revolution, recognizing the potential of AI to drive economic growth, improve public services, and to enhance the quality of life. In this context, the biggest challenge is to provide a legislative frame, concerning compliance and the risk associated with no-compliance. The EU aims to create a framework and to take a proactive approach of AI regulation that ensures the safe and ethical use of AI technologies. AI act represents one of the cornerstone legislative measures, representing the world's first comprehensive law on AI[1]. One of the main purposes is to promote innovation and trust, by establishing rules and standards, I a clear manner, expecting to boost public and business confidence in AI technologies,

[1] European Commission, *Artificial Intelligence in the European Commission,* Brussels, 2024, https://commission.europa.eu/system/files/2024-01/EN%20Artificial%20Intelligence%20in%20the%20European%20Commission.PDF (19.11.2024)

accelerating the integration and adoption into various sectors[1]. Non-compliance can also lead to significant reputational damage. In an era where consumers and stakeholders are increasingly concerned about ethical practices, being found in violation of AI regulations can harm an organization's public image and erode trust[2]. Ensuring compliance with the AI Act requires organizations to implement robust governance frameworks, conduct regular audits, and maintain detailed documentation of their AI systems. This can be resource-intensive and may require significant changes to existing processes and systems[3].

AI theoretical and historical frame

Artificial intelligence is defined as a subfield of computer science dedicated to the exploration of computer capabilities that exhibit behaviors analogous to those of humans. The inception of AI signifies a pivotal advancement in the technological evolution of humanity. Initial concepts of AI emerged in the 1950s, with subsequent technological progress accelerating developments in this domain. The origins of artificial intelligence can be traced back to Alan Turing[4], a prominent logician and computing pioneer. In 1935, Turing published a foundational paper detailing the design of a computational machine characterized by unlimited memory and a memory-guided scanning mechanism capable of generating symbols. This scanner was intended to be directed by a set of symbolic instructions. Turing's contribution is encapsulated in what is now known as the Turing machine, and contemporary computers are widely recognized as universal Turing machines. During the Second World War, Turing was engaged in the clandestine code-breaking efforts at Bletchley Park, under the auspices of the UK government. In 1947, Turing delivered a notable public lecture in London, wherein he posited that computerized intelligence possesses the capacity to learn from experience and adapt its own operational instructions. In 1948, he further elaborated on several AI concepts in a report titled “Intelligent Machines,”making references to chess as a critical domain of application. Starting in 1950, Turing established foundational frameworks for the consideration of machines capable of simulating human intelligence, culminating in the formulation of the Turing test.

The Turing test involves a computational entity and two human participants: an interrogator and a respondent. The interrogator poses questions to both entities, striving to discern which responses originate from the computer. Interaction is facilitated through keyboard and screen, with the interrogator issuing detailed inquiries, while the computer may provide misleading responses. The objective of the Turing test is to evaluate whether a computer can emulate human-like cognitive processes. When the interrogator is unable to differentiate between the computer and the human respondent, the computer is deemed intelligent, thereby successfully passing the test. In contemporary contexts, the Turing test serves as a criterion for assessing AI applications, particularly in domains such as voice recognition and image analysis.

The term “artificial intelligence” was formally introduced in 1956 during the Dartmouth Summer Conference[5], where scientist John McCarthy from the Massachusetts Institute of Technology articulated the concept, marking the commencement of a new technological epoch. AI endeavors to replicate human[6] cognitive abilities in reasoning, context comprehension, generalization, and experiential learning. AI systems can simulate specific human-like behaviors, encompassing planning, problem-solving, perception, manipulation, social intelligence, and creativity.

Initial developments in AI were characterized by the creation of programs aimed at simulating logical processes and problem-solving capabilities. Over time, the advent of machine learning algorithms and neural networks has enabled computers to assimilate information and enhance their performance through experiential

---

[1] European Commission, *Artificial Intelligece – Questions and Answers*, Bruselles, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_21_1683/QANDA_21_1683_EN.pdf (19.11.2024)

[2] *Idem*

[3] European Commission, *Artificial Intelligence in the European Commission,* Brussels, 2024, https://commission.europa.eu/system/files/2024-01/EN%20Artificial%20Intelligence%20in%20the%20European%20Commission.PDF (19.11.2024)

[4] https://www.britannica.com/biography/Alan-Turing (20.10.2024)

[5] J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, *A proposal fot the Dartmouth Summer Research Project on Artificial Itelligence*, https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth (21.10.2024)

[6] Elena Lazar, *The Law of Artificial Intelligence: A Brief Introduction*, Hamangiu Publishing House, Bucharest, 2024, pp. 22-28

learning. Pioneers such as Alan Turing and John McCarthy have significantly contributed to the establishment of fundamental AI concepts. Early AI programs sought to emulate human cognitive processes, exemplified by the "Logic Theorist" program developed by Allen Newell and Herbert A. Simon, which was capable of resolving mathematical problems. The subsequent evolution of AI saw the emergence of rule-based systems (expert systems) designed to replicate human expertise within specific domains. These systems found utility in various applications, including medical diagnosis and decision support mechanisms. Post-1990, advancements in machine learning techniques introduced new paradigms within AI, with support vector machines (SVM) and decision trees gaining prominence.

Since the year 2000, AI applications have increasingly permeated everyday life, with search engines, online product recommendations, and virtual assistants becoming integral components of user experiences. The rise of deep learning and advanced algorithms following 2010 has yielded successful applications in voice recognition, computer vision, and machine translation. At present, AI is pervasive across numerous fields, encompassing healthcare, autonomous vehicles, cybersecurity, intelligence analysis, and beyond. The continuous refinement of algorithms and technologies is propelling AI towards novel challenges and opportunities. AI encompasses a diverse array of components, including expert systems, natural language processing, neural networks, fuzzy systems, genetic algorithms, and robotics. Expert systems are designed to facilitate computer responses in real-world scenarios, such as diagnosing diseases based on symptomatic inputs. Natural language processing endeavors to decode human language, while neural networks replicate cognitive functions by mirroring neural connections observed in biological systems. Fuzzy systems leverage logical frameworks, and genetic algorithms are inspired by Darwinian principles of evolution.

Traditionally, computers have not been equipped to emulate human behavior. However, with the advancements in AI, there is a concerted effort to achieve increasingly accurate simulations. A prominent example of a robot endowed with AI capabilities is Sophia, developed by a Hong Kong-based company; she is capable of mimicking human facial expressions, engaging in conversation, and responding to inquiries. Nonetheless, despite significant advancements, robots still encounter challenges in object identification through visual data and lack the tactile abilities necessary for physical interaction with objects.

The quintessential human capability is thought. Human intelligence is engaged in a competitive landscape with artificial intelligence; despite the capacity of robots to execute specific tasks swiftly and efficiently, AI does not comprehend information in the same manner as humans do. AI facilitates machine translation across diverse languages; however, these translations often lack the precision and comprehensiveness achievable by human translators. Furthermore, numerous applications convert audio to text but do not possess the ability to interpret the content, rendering them useful primarily for dictation purposes. In the realm of artificial intelligence, neural networks are extensively employed in voice recognition and natural language processing applications. In Romania, the Special Telecommunications Service is seeking to implement AI to enhance response times for emergency calls and establish a speech recognition system. AI applications predominantly utilize programming languages such as LISP and Prolog, which are recognized as foundational languages of artificial intelligence. Based on their capabilities and functionalities, artificial intelligence can be categorized into several distinct types:

Narrow AI (ANI)**:** Often referred to as narrow artificial intelligence, this type focuses on the precise execution of specific tasks. Examples include virtual assistants like Siri and Alexa, which understand and respond to vocal commands. Narrow AI is applied in e-commerce for personalized product recommendations and in healthcare for diagnostic purposes utilizing AI tools. General AI[1] (AGI)**:** Known as artificial general intelligence[2], this type represents the aspiration to develop AI systems that can emulate human learning and understanding capacities. AGI applications are not yet operational, but they hold potential for future applications in healthcare (such as drug discovery) and autonomous vehicles capable of navigating complex traffic scenarios.

Superintelligence (ASI)**:** Currently a theoretical construct, superintelligence is posited to exceed human cognitive capabilities and could be employed in advanced scientific research.
In terms of functionality, AI can be divided into several categories:

[1]University of Illinois Chicago, *What is (AI) Artificial Intelligence*, https://meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/ (20.10.2024)

[2] Akash Takyar, *Artificial General Intelligence: Key Insights and Trends, Leeway Hertz*, 2024 https://www.leewayhertz.com/artificial-general-intelligence/ (21.10.2024)

Reactive Machines: These AI systems lack the ability to learn from experience and are designed for rapid decision-making in specific contexts, as exemplified by IBM's[1] Deep Blue chess program.

Limited Memory**:** These systems can comprehend human intentions and emotions, as demonstrated by chatbots and virtual assistants in customer service environments.

Theory of Mind**:** Advanced AI systems within this category possess a nuanced understanding of emotions, enabling applications in mental health therapy or interactions with elderly and disabled individuals.

Self-awareness**:** The most advanced theoretical AI system, characterized by self-awareness, remains largely within the domain of science fiction.

The European Council characterizes artificial intelligence as the application of digital technologies to create systems capable of performing tasks that typically necessitate human intelligence. The European Union endorses the development of AI technologies while acknowledging the associated risks and advocating for ethical, human-centered approaches. The EU intends to prohibit the use of AI in scenarios deemed to pose unacceptable risks, including behavioral manipulation, predictive policing, emotion recognition in workplace settings, educational institutions, and social behavior assessments. Furthermore, remote biometric identification systems, such as facial recognition technologies, will face prohibitions, albeit with certain exceptions. The categories of AI delineated by the European Council encompass software-based AI (represented by virtual assistants, search engines, and systems for voice and facial recognition) and embedded AI (exemplified by robots, autonomous vehicles, and drones). AI aspires to decode the intricacies of thought by constructing mathematical models and computational systems that link logical reasoning with experiential learning, thus achieving an understanding of events akin to human cognition.

In conclusion, artificial intelligence represents the evolution of algorithms and models that empower machines to perceive their surroundings and initiate appropriate actions to fulfill designated objectives. These algorithms leverage vast datasets and employ advanced techniques such as machine learning, deep learning, natural language processing, and computer vision. Andreas Kaplan and Michael Haenlein classify AI into three distinct systems: analytical AI, human-inspired AI, and humanized AI. Analytical AI possesses characteristics akin to cognitive intelligence, generating a cognitive representation of the environment and employing prior experiences to inform future decision-making. Human-inspired AI incorporates elements of both cognitive and emotional intelligence, enabling comprehension of human emotions and their incorporation into decision processes. Humanized AI encompasses all forms of competencies, including cognitive, emotional, and social intelligence, demonstrating self-awareness both and in interactions with others.

AI opens numerous avenues for intelligence analysis, enhancing the objectivity and data-driven nature of insights while mitigating cognitive biases that may arise from human analysts. By employing AI, the data collection process can be automated, allowing human analysts to redirect their focus toward more intricate and creative dimensions of intelligence analysis.

Furthermore, AI's capacity for threat detection, analyzing substantial volumes of data across extensive temporal and spatial parameters, proves invaluable in identifying potential security threats, including cyberattacks and terrorism, thereby facilitating the implementation of preventive measures.

AI systems are adept at analyzing and processing information with greater efficiency than humans, offering profound insights into emerging threats.

Moreover, AI enables the deployment of autonomous systems, such as drones, submarines, and unmanned vehicles, facilitating identification, monitoring, and action with a reduced risk to human operators. AI applications are widely utilized in various security-related domains, particularly in identity protection, cloud security, personal data safeguarding, cyber threat detection, investigative processes, and incident response formulation. Artificial Intelligence (AI) has become an essential pillar of technological innovation in the European Union, significantly impacting the economy, society, and security. In the context of the rapid advancement of AI-based technologies, the European Union has adopted a proactive approach to regulating this field, establishing legislative standards aimed at ensuring the ethical and safe use of these technologies. Artificial Intelligence (AI) refers to the capability of systems or machines to perform tasks that typically require human intelligence. These tasks include, among others, processing information, learning from past experiences, speech recognition, data analysis, decision-making, and interaction with users. AI technologies

[1] Tim Mucci, Cole Stryker, *What is Artificial Intelligence*, https://www.ibm.com/topics/artificial-superintelligence/ (22.10.2024)

can analyze large volumes of data (Big Data) in a short time, interpreting written texts through methods similar to human processes (natural language processing - NLP), identifying threats through machine learning, and deep learning.

Moreover, AI enables the automation of time-consuming repetitive tasks, can anticipate future events through predictions, and can detect anomalies in data, thereby contributing to the development of appropriate responses to threats. The European Union's approach to AI emphasizes excellence, trust, respect for fundamental rights, the promotion of research, and ensuring safety. This approach will influence the future of the world we live in. To build a resilient Europe in the digital age, it is essential that citizens, institutions, and businesses benefit from AI in a safe manner. The European strategy for AI highlights the importance of human-centricity and trust, implementing concrete norms and measures. Within the Digital Strategy[1], the European Union has sought to regulate the use of innovative AI technologies, ensuring that they are used responsibly. Starting in 2021, the European Commission[2] proposed a regulatory framework for the use of AI, aiming to assess and classify AI systems based on the level of risk they present to users. The priority of the European Parliament is to guarantee that AI systems in the European Union are safe, transparent, non-discriminatory, and environmentally friendly.

To prevent harmful effects, the use of AI must be monitored by humans, rather than through automated processes. The AI Act[3] establishes specific rules for each level of risk associated with the use of these technologies. AI systems are classified based on their risk level: unacceptable, high, and limited[4]. Systems posing unacceptable risks, which threaten human safety, will be banned. This includes behavioral manipulation of individuals or classifying them based on personal characteristics, such as social scoring.

Facial recognition[5] and biometric systems fall into the same category. There are exceptions for the use of biometric systems for legal purposes, but these require court approval.

Biometric[6] identification systems can be used in cases of serious crimes, but under strict legal conditions. High-risk AI systems affect safety and fundamental rights. They are divided into two categories: those regulated by EU product safety legislation (e.g., aviation, medical devices) and those from specific fields registered in the European Union database (e.g., critical infrastructure management, education). All high-risk systems will be assessed before being introduced to the market and throughout their entire lifecycle. Generative AI, such as ChatGPT, must comply with transparency requirements, including disclosing that content was generated by AI and avoiding the generation of illegal content.

Low-risk AI systems, such as deepfakes, must meet minimum transparency requirements to inform users. Following interactions with applications, users can decide whether to continue using them. The European Parliament recognizes AI as both a threat and a useful tool in combating cyberattacks. The European Union Agency for Cybersecurity (ENISA)[7] will develop an action plan to assess specific threats related to AI. In March 2024, the European Parliament adopted the first law regulating the use of artificial intelligence, aiming to protect fundamental rights and stimulate innovation. The law will come into effect in 24 months and bans on improper uses will be applicable within six months. The goal is to protect fundamental rights, democracy, and the environment while encouraging innovation in AI. Legislation prohibits the use of AI in ways that affect citizens' rights, such as exploiting sensitive personal characteristics. The extraction of facial images from video recordings or the online environment for the purpose of creating facial recognition

[1]European Union Agency for Cybersecurity. *Multilayer Framework for Good Cybersecurity Practices for AI*, June 2023, https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai (24.10.2024)

[2] European Commission, *Shaping Europe`s Digital Future*, https://digital-strategy.ec.europa.eu/en/policies/ai-people/ (22.10.2024)

[3]Deloitte, *Legea UE privind inteligența artificială. O analiză amănunțită*, https://www2.deloitte.com/ro/ro/pages/about-deloitte/articles/eu-artificial-intelligence-act-deep-dive.html (22.10.2024)

[4]Parlamentul European, Legea UE privind IA: prima reglementare a inteligenței artificiale, https://www.europarl.europa.eu/topics/ro/article/20230601STO93804/legea-ue-privind-ia-prima-reglementare-a-inteligentei-artificiale (23.10.2024)

[5]Eastern Romanian Business Suport Network, *Legea inteșigenței artificiale a fost adoptată de Parlamentul European,* https://een-erbsn.ro/noutati/legea-inteligentei-artificiale-a-fost-adoptata-de-parlamentul-european/ (23.10.2024)

[6] G4Media, *Legislație AI*, https://www.g4media.ro/tag/legislatie-ai (23.10.2024)

[7] Eastern Romanian Business Suport Network, *Legea inteligenței artificiale a fost adoptată de Parlamentul European,* https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai, (24.10.2024)

databases is prohibited. Judicial authorities may use biometric identification under clear and strictly regulated conditions.

Real-time biometric identification systems require approval, while post-event systems are used under judicial authorization. Citizens may file criminal complaints if high-risk AI systems violate their rights. It is essential for AI to comply with transparency norms and EU copyright legislation. Images and content generated by AI must be properly labeled, and member states must establish regulatory testing spaces. The EU AI Act aims to mitigate risks and create opportunities, ensuring the protection of citizens' rights. In cases of non-compliance with the legislation, significant fines will be imposed, reaching up to 7% of global[1] revenue. By adopting this law, the intention is to reduce risks and increase transparency in the use of artificial intelligence in the European Union. The effects of the law will apply directly in all member states, and updates will be made through amendments to the annexes of the regulation.

The establishment of the Artificial Intelligence Regulatory Authority is a direct consequence of implementing the AI Act. It is essential to create a body that facilitates the application of the specifications of this act, including participation in regulated testing spaces. The European Commission has decided to establish an Office for Artificial Intelligence[2], aimed at strengthening the European Union's leadership position in the field of artificial intelligence. The purpose of this office is to promote the development and use of AI technologies, emphasizing societal and economic benefits while mitigating associated risks. The office will ensure compliance with legislation related to artificial intelligence and stimulate research and innovation in this field, thereby contributing to increased trust in technology.

At the national level, Romania will establish a Coordination Committee for the application of European regulations in the fields of data, digital services, and artificial intelligence. The government has approved, through a memorandum, the establishment of this committee, which will be responsible for monitoring and controlling aspects related to data, digital services, and artificial intelligence.

The committee[3] will include representatives from various institutions, such as: the National Authority for Management and Regulation in Communications, which will oversee the implementation of the Digital Services Regulation (DSA) to ensure safety and fairness in the online environment; the Ministry of Research, Innovation, and Digitalization, which supports the digitalization of public institutions; the Romanian Authority for Digitalization (ADR), which facilitates the implementation of the government cloud infrastructure project through the National Recovery and Resilience Plan[4] (NRRP- PNRR in Romanian language); the National Supervisory Authority for Personal Data Processing; the National Cyber Security Directorate; the National Institute of Statistics (INS); the National Authority for Consumer Protection; the National Audiovisual Council and the Competition Council. By establishing this committee, national cooperation will be promoted to achieve the following objectives:

- Implementing and enforcing relevant legislation, clearly defining responsibilities, especially for interdependent ones;
- Harmonizing the interpretation of existing and future European norms;
- Coordinating market interventions according to specific responsibilities;
- Ensuring compliance with decisions adopted by the parties involved regarding identified issues;
- Exchanging information, advice, and recommendations regarding the implementation and compliance with European norms;
- Organizing events for the exchange of experiences, including meetings with industry representatives and service providers.

Committee members will collaborate in the fields of data management and reuse, defining standards and norms compliant with European legislation, especially in the context of artificial intelligence. Guidelines and recommendations for best practices will be developed, adopting common positions on relevant regulations

[1] *EU Artificial Intelligence Act*, https://artificialintelligenceact.eu/article/99/ (22.10.2024)

[2] Autoritatea pentru Digitalizarea României, *Strategia națională în domeniul inteligenței artificiale 2024-2027*, https://sgg.gov.ro/1/wp-content/uploads/2024/07/ANEXA-1-10.pdf (22.10.2024)

[3] *Cum se pregătește România să țină sub control inteligența artificială?,* https://legalbadger.org/stiri/social/cum-se-pregateste-romania-sa-tina-sub-control-inteligenta-artificiala/ (22.10.2024)

[4] G4Media, *România va avea un comitet de coordonare pentru date, servicii digitale și inteligență artificială,* https://www.g4media.ro/romania-va-avea-un-comitet-de-coordonare-pentru-date-servicii-digitale-si-inteligenta-artificiala.html (22.10.2024)

and promoting them in working groups at the European level. Regarding the legal framework for artificial intelligence, the European Commission aims to support the creation of a regulatory environment favorable to the development of this technology while respecting the fundamental values of the European Union.

The approach to a dedicated legislative act for artificial intelligence requires caution, which has led the European Commission[1] to form a group of experts in responsibility for new technologies and social challenges to develop principles that will guide legislative adaptations at the European and national levels.
AI engineering experts must take responsibility for the social and environmental impact of artificial intelligence systems on current and future generations. AI thus becomes an essential tool for collaboration with human action, aiming to reduce errors.

The European Parliament seeks to ensure citizens' access to knowledge, the right to challenge, and compensation for harm caused using artificial intelligence. The European Union is at the forefront of legislative initiatives regarding the use of artificial intelligence, aiming to regulate this field through an ethical, safe, and trustworthy approach. The EU AI Act represents the first legal framework designed to ensure the security of AI systems and compliance with the legislation and fundamental values of the Union. Decision-making system algorithms must not be implemented without prior impact assessment, except in cases where the impact on people's lives is negligible. The European Parliament emphasizes that the use of artificial intelligence, particularly autonomous systems capable of extracting, collecting, and sharing sensitive information, must adhere to strict principles. These systems must not retain or disclose confidential information[2] without the explicit consent of the respective source. The legislative benefits provided by artificial intelligence are numerous.

Innovation and economic growth. Clear regulations aim to stimulate innovation, thus providing a framework of trust for investments. Legally supported AI projects can lead to the creation of new jobs and streamline economic processes. AI-based technologies can foster innovation across various sectors, including health, education, and transportation. For example, AI can improve medical diagnosis through advanced data analyses, thereby contributing to the discovery of new treatments and medications.

Protection of citizens' rights. Regulations such as GDPR[3] (General Data Protection Regulation) represent the way the European Union has set out to protect citizens' personal data, promoting an environment for AI development that respects fundamental rights. This contributes to increasing citizens' trust in technology[4]. European legislation[5] emphasizes the protection of individual fundamental rights. By imposing transparency and accountability requirements, regulations ensure that the use of AI respects democratic principles and does not discriminate.

Responsibility and ethics. AI legislation encourages the development of ethical solutions that consider social and moral impact. EU initiatives to define ethical[6] principles for AI help to prevent abuses. Standardization and Interoperability. The establishment of common standards at the European level ensures that AI technologies are compatible and can be easily integrated into various sectors, leading to increased efficiency. Fostering international cooperation. Through a united legislative approach, the European Union can position itself as a leader in AI, promoting international collaboration on norms and ethical standards. The European Union's regulatory framework for artificial intelligence serves not only to protect its citizens but also to set a global benchmark for ethical AI practices. By actively engaging with international partners, the EU

---

[1] European Commission, *High-level Expert Group on Artificial Intelligence,* https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai/ (23.10.2024)

[2]European Parliament, *EU AI Act: First Regulation on Artificial Intelligence,* https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence/ (23.10.2024)

[3] InfoCons, *Cum funcționează inteligența artificială,* https://infocons.ro/cum-functioneaza-inteligentan-artificiala/ (23.10.2024).

[4]Comitetul European al Regiunilor, *Liderii locali se mobilizează pentru a pune inteligența artificială în slujba cetățenilor prin intermediul unor servicii îmbunătite,* https://cor.europa.eu/ro/noutati/liderii-locali-se-mobilizeaza-pentru-pune-inteligenta-artificiala-slujba-cetatenilor-prin (23.10.2024)

[5]European Council, *Artificial Intelligence (AI) Act: Council gives final green light to the first world wide rues on AI,* https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ (23.10.2024)

[6] European Law Blog, *When EU Data Protectioan Meets AI Tools – The CJEU determines responsibility,* https://www.europeanlawblog.eu/pub/hg7qrggl/release/1?readingCollection=65b658d5 (23.10.2024)

aims to promote shared values and standards in AI governance, ensuring that advancements in technology align with human rights and ethical considerations.

Challenges and future Directions. While the establishment of the EU AI Act represents a significant step forward, challenges remain in its implementation and enforcement. Ensuring compliance across diverse member states, addressing rapidly evolving technology, and maintaining a balance between innovation and regulation will be critical. Continuous dialogue between stakeholders—including governments, industry leaders, researchers, and civil society—will be essential for adapting the regulatory framework to emerging challenges. Moreover, education and awareness-raising initiatives are crucial to equip citizens with the knowledge needed to navigate an AI-driven world. This includes understanding their rights regarding AI technologies, the implications of data privacy, and how to engage with AI systems responsibly.

Conclusions

European legislation regarding artificial intelligence has the potential to radically transform the technological landscape, providing significant benefits to society. By establishing clear and comprehensive standards, the European Union aims to maximize the advantages that AI can offer, while simultaneously encouraging responsible innovation and safeguarding the fundamental rights of citizens. This legislative approach not only stimulates economic and social development but also ensures an ethical framework within which emerging technologies can be utilized beneficially.

However, non-compliance with established norms can have serious consequences, including risks to the fundamental rights of citizens. For instance, the abusive use of facial recognition technologies or predictive algorithms may lead to discrimination, invasions of privacy, and the erosion of trust in democratic institutions. Furthermore, inadequate implementation of regulations may destabilize the market, favoring uncontrolled innovation and amplifying economic inequalities.

Therefore, it is essential for stakeholders in the artificial intelligence sector to closely collaborate with authorities to ensure compliance with regulations and to maximize the benefits of this innovative technology. Such collaboration can facilitate constructive dialogue between industry and legislators, ensuring that the perspectives and needs of each party are integrated into the legislative framework. The benefits[1] of artificial intelligence often outweigh the challenges and risks associated with its use, including imposed sanctions and regulations. With a well-defined legal framework, companies can innovate with confidence, assured that they are adhering to ethical and legal standards. This not only enhances the brand reputation but also fosters healthy competition in the marketplace.

Artificial intelligence within the European Union presents considerable opportunities for economic and social development, but it is essential that these technologies be appropriately regulated. Legislative benefits, including the protection of fundamental rights and the promotion of responsible innovation, are fundamental to ensuring the ethical use of AI. At the same time, the challenges associated with non-compliance with legislative norms underscore the importance of rigorous implementation of existing regulations. Only through a coordinated and responsible approach can it be ensured that artificial intelligence will positively contribute to the future of European society, creating an environment where technology and human values coexist harmoniously.

As a conclusion, the stringent penalties for non-compliance with the European Union's regulations regarding the use of artificial intelligence should be viewed as a crucial mechanism for safeguarding public interest, promoting ethical practices, and ensuring accountability among AI developers and users.
These sanctions serve not only as a deterrent against potential misuse but also to uphold fundamental rights and prevent harm to individuals and society.

Given the rapid evolution of AI technologies and their profound implications, there is a compelling argument for considering even stricter enforcement measures. Enhanced penalties could reinforce the seriousness of compliance, ensuring that organizations prioritize ethical considerations and adhere to established norms. Such an approach would signal a robust commitment to responsible AI deployment, fostering a culture of accountability that ultimately benefits both society and the technology sector. However, any decision to further intensify sanctions must be balanced with an understanding of the potential impact on innovation.

[1] Elle Glover, *What is Artificial Intelligence (AI)?*, https://builtin.com/artificial-intelligence/ (21.10.2024)

It is essential to create a regulatory environment that encourages responsible innovation while effectively mitigating risks. Thus, ongoing dialogue among stakeholders—including policymakers, industry leaders, and civil society—is vital to refine these regulations and their enforcement mechanisms, ensuring they are both effective and conducive to a sustainable technological landscape.

Bibliography

Books

1. Bontcheva, Kalina; (Ed.), *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunites*, University of Sheffield, 2024
2. Chowdhary, K.R. *Fundamentals of Artificial Intelligence*, Springer Nature Indi Private Limited, New Dehli, 2020
3. Lazăr, Elena, *The Law of Artificial Intelligence: A Brief Introduction*, Hamangiu Publishing House, Bucharest, 2024

Documents

1. Autoritatea pentru Digitalizarea României, *Strategia națională în domeniul inteligenței artificiale 2024-2027*, https://sgg.gov.ro/1/wp-content/uploads/2024/07/ANEXA-1-10.pdf
2. Comitetul European al Regiunilor, *Liderii locali se mobilizează pentru a pune inteligența artificială în slujba cetățenilor prin intermediul unor servicii îmbunătite,* https://cor.europa.eu/ro/noutati/liderii-locali-se-mobilizeaza-pentru-pune-inteligenta-artificiala-slujba-cetatenilor-prin
3. Eastern Romanian Business Suport Network, *Legea inteligenței artificiale a fost adoptată de Parlamentul European,* https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai
4. Eastern Romanian Business Suport Network, *Legea inteligenței artificiale a fost adoptată de Parlamentul European,* https://een-erbsn.ro/noutati/legea-inteligentei-artificiale-a-fost-adoptata-de-parlamentul-european
5. *EU Artificial Intelligence Act*, https://artificialintelligenceact.eu/article/99/
6. European Commission, *Artificial Intelligence in the European Commission*, Brussels, 2024, https://commission.europa.eu/system/files/2024-01/EN%20Artificial%20Intelligence%20in%20the%20European%20Commission.PDF European Commission, *Shaping Europe`s Digital Future*, https://digital-strategy.ec.europa.eu/en/policies/ai-people/
7. European Council, *Artificial Intelligence (AI) Act: Council gives final green light to the first world wide rues on AI*, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/
8. European Law Blog, *When EU Data Protection Meets AI Tools – The CJEU determines responsibility*, https://www.europeanlawblog.eu/pub/hg7qrggl/release/1?readingCollection=65b658d5
9. European Parliament, *EU AI Act: First Regulation on Artificial Intelligence,* https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
10. European Union Agency for Cybersecurity, *Multilayer Framework for Good Cybersecurity Practices for AI*, June 2023, https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai
11. InfoCons, *Cum funcționează inteligența artificială,* https://infocons.ro/cum-functioneaza-inteligentan-artificiala/
12. Parlamentul European, *Legea UE privind IA: prima reglementare a inteligenței artificiale*, https://www.europarl.europa.eu/topics/ro/article/20230601STO93804/legea-ue-privind-ia-prima-reglementare-a-inteligentei-artificiale

Websites

1. https://artificialintelligenceact.eu/
2. https://builtin.com/
3. https://cor.europa.eu/ro/

4. https://digital-strategy.ec.europa.eu/
5. https://een-erbsn.ro/
6. https://infocons.ro/
7. https://legalbadger.org/
8. https://meng.uic.edu/
9. https://sgg.gov.ro/
10. https://www.consilium.europa.eu/
11. https://www.enisa.europa.eu/
12. https://www.europarl.europa.eu/
13. https://www.europeanlawblog.eu/
14. https://www.g4media.ro/
15. https://www.ibm.com/
16. https://www.leewayhertz.com/
17. https://www2.deloitte.com/

Cristina EJOVA
Moldova State University, Republic of Moldova

ANALYSIS OF THE CONCEPT OF CYBERTERRORISM IN THE CONTEXT OF POLITICAL SCIENCE

Abstract:	*This paper examines the concept of cyberterrorism through the lens of political science, focusing on its origins, development, and impact on global security. With the exponential growth of information technology, cyberterrorism has emerged as a significant threat, utilizing advanced technological means to destabilize political and social frameworks. The rapid increase in internet access has introduced new opportunities for both communication and crime, including the use of digital platforms for extremist and terrorist activities.* *The study emphasizes the complex methodologies required for analyzing cyberterrorism, including systemic, institutional, and comparative approaches, each contributing to a nuanced understanding of this phenomenon. Based on a systemic approach, the specifics of various definitions of the phenomenon of "cyberterrorism" will be revealed. It is argued that modern cyberterrorism, aimed at creating threats to international and national security, serves as one of the effective tools for achieving political goals on the global stage. Utilizing theories such as the information society and network society, the article underscores the importance of international cooperation in combating cyberterrorism.*
Keywords:	**Cyberterrorism; cyberspace; cyber-attack; Internet; information society**
Contact details of the authors:	E-mail: cristina.ejova@usm.md
Institutional affiliation of the authors:	**Department of International Relations, Faculty of International Relations Political and Administrative Sciences, Moldova State University, Republic of Moldova**
Institutions address:	Moldova State University, 60 A. Mateevici Str., Chișinău, http://usm.md

Introduction

The modernization of society and the development of information technologies have led to the widespread use of the Internet worldwide, giving rise to one of the most dangerous forms of cybercrime – cyberterrorism, which utilizes the latest advancements in science and technology. The twenty-first century can confidently be called the century of information technologies, due to their constant development and integration into our lives. The emergence of global informatization has resulted in the creation of a unified information space – the World Wide Web and new ICT tools. More than 66% of the world's population uses the Internet, and according to the latest data, the total number of Internet users globally amounts to 5.35 billion. Over the past 12 months, the Internet audience has grown by 1.8% (97 million new users since the beginning of 2023)[1]. However, the rapid expansion of the digital realm has created opportunities for exploitation by extremist and terrorist

[1] *Digital 2024: Global Overview Report*, https://indd.adobe.com/view/8892459e-f0f4-4cfd-bf47-f5da5728a5b5 (02.04.2023)

organizations, which use these platforms to disseminate propaganda, recruit members, and even operational planning.

A prominent illustration of this phenomenon is the online presence and activities of the terrorist group "Islamic State of Iraq and the Levant" (ISIS). In 2014, ISIS disseminated a documentary titled *The Clanging of the Swords* via global online platforms, serving as a potent instrument of psychological propaganda. The film depicted brutal scenes of ISIS armed forces' combat actions against the government troops of Syria and Iraq, bloody massacres of civilians, and the families of military personnel. This content was created to intimidate and spread extremist ideology.

The group also capitalized on the video game industry by developing a modified version of the popular game Grand Theft Auto (GTA), named GTA–ISIS: The Jihad Simulator, which integrated their ideology. Social media has proven to be another essential tool for ISIS. The group used part of the technological infrastructure of global social networks to actively propagate on behalf of the "Islamic State" on platforms as "VKontakte" and others. These platforms not only served as channels for content dissemination but also played a key role in the recruitment of new members.

The dual nature of the development of information and communication technologies underscores the urgent need for the development of comprehensive strategies to monitor, regulate, and counter the misuse of digital spaces by such organizations.

The influence of global networks on the socio-political development of society is multifaceted and contradictory. On the one hand, they contribute to the development of human potential through computer games, educational and entertainment programs, interactive television, and electronic media. Global networks also impact the electoral behavior of political actors, the organization and conduct of election campaigns, mechanisms of communication between the government and society, as well as the presentation and advocacy of political actors' interests. On the other hand, the rapid development of the information and communication sphere has led to the emergence of new types of crimes – computer crime and cyberterrorism. Some notable examples have been recorded in the past years.

In recent years, cyberattacks have an alarming increase on a global scale. According to a report published in 2024 by Check Point Research, the number of cyberattacks worldwide has risen by approximately 30% over the past two years, highlighting a dangerous trend in the advanced use of technology by malicious entities. This situation not only amplifies risks but also increases the probability that terrorist groups and organizations will utilize cutting-edge technologies to commit actions bearing the hallmark of terrorism or to achieve terrorist objectives[1]. A relevant example is the cyberattacks of 2024. In January 2024, while Sweden was preparing to join NATO, a ransomware attack was launched on the governmental digital service. The attack, carried out by a Russian hacker group, disrupted the functioning of 120 government offices[2]. Just six months later, a Microsoft Windows update led to a global IT outage, interrupting the operations of airlines and hospitals[3].

Although the incident was caused by a malfunctioning software update, it exposed users, both individuals and private companies, to additional planned attacks. Around 8.5 million machines were affected, resulting in a loss of $5.4 billion for Fortune 500 companies[4]. In 2021, the Center for Strategic and International Studies (CSIS) identified 118 cyberattacks that could be classified as acts of cyberterrorism. These attacks targeted government institutions, major information technology

[1] Check Point, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks*, July 2024, https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/ (26.11.2024)

[2] Center for Strategic and International Studies, *Significant Cyber Incidents* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (26.11.2024)

[3] *Idem*

[4] *Idem*

companies, and defense industry enterprises. Among the incidents were cyberattacks on major critical infrastructure facilities such as the water supply system in Oldsmar, Florida; Poland's National Atomic Energy Agency; Poland's Ministry of Health, and several others. Since 2023 the Center has recorded over 800 cases, underlying the severity of the situation and the vulnerability of governments and individuals in the digital sphere[1].

The activities of cyberterrorists in virtual space can harm thousands of network users, not only individuals but entire states. Global informatization processes and the development of information technologies have led to the creation of a new platform for criminal activity, which requires new approaches to ensuring security.

Methodological approaches to research

The study of cyberterrorism presents a complex scientific challenge due to the multifaceted nature of this phenomenon, which encompasses political, social, psychological, and technical aspects. This issue cannot be confined to a single definition and requires an interdisciplinary approach, involving political science, sociology, psychology, law, information technology, and other fields. The rapid development of information and communication technologies adds complexity to the study of cyberterrorism, as this process impacts virtually all areas of modern society. The main methodological approaches in cyberterrorism research include *systemic, institutional, structural-functional,* and *comparative approaches*. Scientific investigation of relevant topics is also carried out through the application of research theories such as information society theory and network society theory.

The systemic approach in researching the phenomenon of cyberterrorism involves viewing it as an integrated and complex issue, which requires recognizing the essential elements of international cooperation for effectively preventing and countering cyber threats. Since cyberterrorism transcends national borders and is characterized by global technological interdependence, its effective counteraction is only possible through strong international collaboration. The systemic approach allows for a deeper understanding of the interactions among actors, infrastructures, and cybersecurity policies, enabling the development of common defense and prevention strategies that provide effective protection against cross-border cyberattacks.

The institutional approach allows for an assessment of how government and specialized institutions (such as the presidency, parliament, and security services) respond to cyberterrorism threats. This study focuses on the structure, functions, and interactions between various organizations to develop coordinated measures to counter cyber threats. The institutional approach also includes the study of other countries' experiences and practices in cybersecurity, enabling consideration of global trends and adaptation of effective international strategies to the national context.

The author has also applied *structural-functional analysis* as methodological support. The method of structural-functional analysis is aimed at solving issues related to maintaining stability, functioning, and viability of the system. The structural component involves identifying the main elements of the system and stable connections between them. In turn, the functional component analyzes the mechanisms of interaction between these elements and determines how the system interacts with the external environment. Understanding the internal interconnections and interactions between system components allows for identifying the conditions necessary for its operability and the influence of external factors on its functioning. Applied to cyberterrorism, this method enables the formation of a counteraction system structure that includes subsystems such as institutional, regulatory-legal, organizational-functional, communicative, human resources, and cultural. This

[1] Center for Strategic and International Studies, *Significant Cyber Events List*, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-11/241114_Significant_Cyber_Events.pdf?VersionId=x077LxbEUZ9.EQb8yEUMcTa5ebhzQHQe (26.11.2024)

approach facilitates a comprehensive analysis and the development of policies to counter cyber threats.

The comparative method in analyzing the phenomenon of cyberterrorism offers a complex perspective, allowing for the comparison of approaches and contributions by Western and Russian authors. This method helps identify differences and similarities in the definition and understanding of the phenomenon, prevention and counteraction strategies, as well as the role of the state and international institutions. Studies by Western authors tend to focus on the technological and critical infrastructure aspects of cyberterrorism, emphasizing the importance of international cooperation and rapid adaptation to new cyber threats. In contrast, Russian authors often emphasize the role of national sovereignty and the need for strict internal regulation in managing cyber risks.

Comparing these perspectives enables a clearer understanding of the priorities and challenges each approach faces. For instance, Western sources extensively explore the development of public policies and public-private partnerships in cybersecurity, whereas Russian authors focus on the direct involvement of the state and government control measures. Thus, the comparative method provides not only a diversity of views on the phenomenon, but also potential solutions tailored to the specific political and social context of each region.

Information society theory. Information society theory, which emerged as part of the post-industrial society concept, emphasizes changes in a society where the production, distribution, and consumption of information take center stage. In such a system, the role of cybersecurity and the protection of information infrastructures increases. Information technologies, on the one hand, facilitate improvements in public policy and crisis management; on the other hand, they can generate new threats, such as cyberterrorism.

Network society theory. Network society theory explains how global social changes in the last decades of the 20th century led to the formation of a new social structure based on network interaction. At the core of this theory are information and communication technologies, which facilitate the active reproduction of knowledge. As the role of global networks (such as the internet, political, and terrorist networks) grows, state structures and power relations also undergo changes, replacing traditional hierarchies with network forms of interaction and decentralized power distribution.

The network society significantly influences socio-political development by fostering constructive interaction between state institutions and society. However, it also introduces new threats, such as cyberterrorism. The theory of the network society provides a framework for analyzing the conditions that facilitate the spread of cyberterrorism through global networks. Moreover, it aids in devising effective countermeasures tailored to the complexities of interconnected digital structures[1].

Definition and specificity of cyberterrorism

The term "cyberterrorism" was first used in 1980 by B. Collin, a specialist at the Institute for Security and Intelligence in California[2]. He used this term to denote the potential for terrorist attacks in cyberspace. At that time, the precursor to the Internet—the ARPANET network of the U.S. Department of Defense's Advanced Research Projects Agency—connected only a few dozen computers within one country. However, the researcher was certain that, although cyber networks would eventually be embraced by terrorists, this development would not happen before the first decade of the 21st century[3]. In the 1980s, this term had not yet materialized and was used as a

[1] Eliot Che, *Securing a Network Society: Cyber-Terrorism, International Cooperation, and Transnational Surveillance,* "Research Paper", No. 113, Research Institute for European and American Studies (RIEAS), Athens, September 2007, pp. 25-26, https://rieas.gr/images/RIEAS113ELIOTCHE.pdf (03.12.2024)
[2] Barry Collin, *The Future of Cyber Terrorism*, "Crime & Justice International", Vol. 13, No. 2, March 1997, p. 16
[3] *Ibidem*, p.18

projected development for the near future. In 1997, FBI special agent Mark Pollitt defined this type of terrorism as "politically motivated attacks on information, computer systems, computer programs, and data, expressed through violence against civilian targets by subnational groups or clandestine agents"[1].

To define the term cyberterrorism, it is also necessary to define the terms terrorism and cyberspace. Cyberspace is a global domain of interconnected and interdependent networks where data is processed, transferred, and stored in machine-readable formats. It encompasses not only a virtual level, including digital systems and programs, but also a physical infrastructure and a human domain that reflects user activities and interactions. This multifaceted space plays a critical role in technological and sociopolitical processes, shaping and being shaped by global dynamics[2].

Terrorism is a complex socio-political phenomenon that represents an act of illegal violence or a threat of using it, deliberately committed by individuals or a group of persons to achieve a political or ideological goal that can be national, transnational, or international in nature. Another key element of terrorism lies in its ability to instill fear in society and intimidate the population to achieve specific political aims. At the same time, the causes of terrorism may be economic, political, religious, or territorial. Contemporary terrorism is marked by the following traits: a complete lack of control by state structures; a hybrid nature, involving a combination of criminal motives and terrorist ideology; rapid transformation; the expansion of the technical capabilities of destructive weapons; increased scope and geographic spread; and strong financial backing[3].

One of the first groups to use the internet for illicit purposes is the "Tamil Tigers" who, in 1998, bombarded Sri Lankan government offices with emails for two weeks, referring to themselves as the "Black Internet Tigers". Around the same time, "Aum Shinrikyo" (as discovered during searches of the organization's headquarters) was working on the possibility of intercepting control over nuclear facilities[4].

The study of cyberterrorism as a scientific discipline has several unique characteristics. First, it is interdisciplinary, encompassing research in political, legal, and technical fields. Second, it is practically oriented, directly addressing challenges related to information security. These factors contribute to a wide range of theoretical approaches applied to understanding this phenomenon.

The international community has not yet developed a unified definition of "cyberterrorism", which makes it difficult to develop effective measures to combat this type of crime. Specialists in international relations and law, as well as representatives of international organizations, face problems in formulating this concept, as well as in distinguishing between the term's "cybercrime" and "cyberterrorism". Unlike cybercriminals, the main goal of terrorist organizations is "inciting international and social tension, stirring up ethnic and religious hatred and enmity, promoting extremist ideology, attracting new supporters through informational influence on individual, group and public consciousness", as well as using means of destructive impact (cyber weapons) on critical information infrastructure objects. However, according to experts, "to date, there has been no

[1] Mark M. Pollitt, *Cyberterrorism: Fact or Fancy?*, "Computer Fraud and Security", February 1998, pp. 8–10

[2] Nick Ebner, *Cyber Space, Cyber Attack and Cyber Weapons A Contribution to the Terminology*, "Institute for Peace Research and Security Policy at the University of Hamburg", Hamburg, October 2015, p. 3, https://epub.sub.uni-hamburg.de/epub/volltexte/2018/80797/pdf/IFAR2_FactSheet7.pdf (02.12.2024)

[3] Cristina Ejova, *Unele abordări conceptuale ale terorismului, "*Studia Universitatis Moldaviae. Științe Sociale", No. 3, 2023, pp. 252-253, https://social.studiamsu.md/wp-content/uploads/2023/05/31_C_Ejova.pdf (15.10.2024)

[4] Galina Kuleshova, Elena Kapitonova, Georgy Romanovsky, *Pravovye osnovy protivodejstviya kiberterrorizmu v rossii i za rubezhom s pozicii obshchestvenno- politicheskogo izmereniya*, "Russian Journal of Criminology", Vol. 14, No. 1, 2020, p. 157, https://cyberleninka.ru/article/n/pravovye-osnovy-protivodeystviya-kiberterrorizmu-v-rossii-i-za-rubezhom-s-pozitsii-obschestvenno-politicheskogo-izmereniya (2.11.2024)

recorded large-scale use of malicious software by terrorist organizations aimed at disrupting the operation of critical information infrastructure"[1].

The lack of a universal definition of terrorism complicates the characterization of cyberterrorism without reference to traditional forms of terrorism. In this regard, let us turn to the opinions of scholars in the field of political science.

In 2000, Professor of Computer Science at Georgetown University, Dorothy Denning, one of the most authoritative experts in cybersecurity, categorized terrorists' activities on the Internet into three groups: activity, hacking, and cyberterrorism. By "activity", she refers to the simple use of computer technologies for the purposes of propaganda, fundraising, and attracting new followers. In this context, cyberspace serves as a means that facilitates the unification of terrorists and the recruitment of new members into terrorist organizations. The online capabilities for collecting donations are vast, ranging from simple transfers of funds through methods indicated on websites.

Hacking refers to illegal attacks on computer networks, secret databases, and websites to obtain information or steal money.

Cyberterrorism is defined by the researcher as "illegal attacks or threats of attacks on computers, networks, and the information stored within them, aimed at intimidating or coercing governments or citizens into taking certain actions for political or social purposes"[2]. The researcher also noted that while cyberterrorism is similar in its implementation methods to hacking, it represents, according to Danning, a distinctly different type of computer attack that involves causing significant damage to critical infrastructure using information technologies[3].

We agree with Danning's position; her classification of terrorist activities in cyberspace into three groups allows for a clearer understanding of the distinctions between types of cyberattacks. It is important to emphasize that it is the political motive and the intent to exert pressure on the government that differentiates cyberterrorism from other forms of illegal activity in the network. This definition helps to highlight the destructive potential of cyberterrorism.

Also, in the 2000s, the German scholar K. Hirschmann, in his work "The Changing Face of Terrorism" defined cyberterrorism as a premeditated, politically motivated attack on information and cyberspace for terrorist purposes, meaning operations aimed at breaking into computer systems, computer programs, and their processing, which take the form of violence against neutral objects by subnational groups or individuals acting clandestinely[4]. Hirschmann, in turn, views cyberterrorism as a consciously planned political attack, where the concealment of actions holds particular significance. Thus, his approach enhances the understanding that cyberterrorist attacks are aimed not merely at disrupting systems but also at destabilizing with a political objective. Researchers M. J. Devost, B. X. Houghton, and N. A. Pollard define cyber-terrorism as:

(1) the combination of criminal use of information systems through fraud or abuse with physical violence characteristic of terrorism; and

[1] UN General Assembly, *Resolution A/54/49: Developments in the Field of Information and Telecommunications in the Context of International Security*, December 1, 1999, https://documents.un.org/doc/undoc/gen/n99/777/13/pdf/n9977713.pdf (02.11.2024)

[2] Dorothy E. Denning, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, May 23, 2000, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm (02.11.2024)

[3] Dorothy E. Denning, *Is Cyber Terror next*?, "Social Science Research Council", https://items.ssrc.org/after-september-11/is-cyber-terror-next/ (02.11.2024)

[4] Kai Hirschmann, *The changing face of terrorism*, „International Politics", No. 3, 2000, p. 308, https://library.fes.de/pdf-files/ipg/ipg-2000-3/arthirschmann.pdf (02.11.2024)

(2) the intentional misuse of digital information systems, networks, or components of those systems or networks for purposes that facilitate the execution of terrorist operations or acts[1].

American researcher K. Wilson defines cyber-terrorism as the use of computers as a weapon or target by politically motivated international or transnational groups, or clandestine agents, who threaten or inflict violence and instill fear to influence or coerce the government to change its policies[2].

According to Dutch researcher Ruben Tuitel, cyber-terrorism is the use of cyberspace by non-state actors to disrupt the functioning of computer systems, instill a sense of fear, or cause physical harm, and indirectly, health damage, or create disruptions that seriously threaten the reputation of the victim, carried out for political, ideological, or religious purposes[3]. We agree with this opinion, as it highlights the multifaceted nature of cyberterrorism and the importance of its political, ideological, or religious orientation.

A well-known expert on cyberterrorism, Professor Gabriel Weiman from the Faculty of Communications at the University of Haifa, defines cyber-terrorism as a specific intersection of cyberspace and terrorism, including illegal cyberattacks or threats of such attacks on information networks aimed at intimidating or coercing the government or its people to achieve political goals. According to Weiman, such classification is only possible if the outcomes lead to serious consequences that instill fear in the population, and attacks on critical infrastructure should be classified based on the damage caused. He identifies several features of cyber-terrorism at the present stage: firstly, cyberattacks are significantly cheaper compared to traditional terrorist methods; secondly, cyberterrorism provides terrorists with a high level of anonymity, complicating security services' efforts to identify them; the global network offers a wide range of targets, allowing effective attacks to be carried out remotely, thereby reducing the need for physical preparation and lowering risks for the perpetrators; additionally, digital attacks can reach a substantial number of users, capturing media attention and amplifying the impact that terrorists aim to achieve[4].

Professor Gabriel Weiman also notes that while the threat of cyberterrorism may be exaggerated, it cannot be ignored [5].

Weiman rightly emphasizes the uniqueness of cyberterrorism, highlighting its specific characteristics, such as anonymity and the remote nature of attacks. Indeed, the potential for covert influence achieved in cyberspace makes cyber-terrorism a powerful tool for political pressure, as evidenced by extensive media coverage of such attacks. At the same time, his warning about the possible exaggeration of the threat of cyberterrorism points out the need for a balanced approach in assessing cyberattacks on critical infrastructure and in developing strategies for their prevention.

Jerome Orji, an expert in cybersecurity and its regulatory framework, a researcher at the African Centre for Cyberlaw and Cybercrime Prevention (ACCP) in Kampala, Uganda, categorizes cyberterrorism as a terrorist attack against or through computers and network infrastructures aimed at disrupting vital sectors and achieving terrorist objectives: loss of life, panic, economic collapse, or intimidation to influence government policy[6].

---

[1] Tat'yana Tropina, *Kiberprestupnost' i kiberterrorizm: pogovorim o ponyatijnom apparate*, in *Informacionnye Tekhnologii i Bezopasnost'*". *Sbornik nauchnyh trudov mezhdunarodnoj konferencii*, Nacional'naya Akademiya Nauk Ukrainy, Kyiv, 2003, pp. 177 – 178

[2] Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues*, October 2003, https://apps.dtic.mil/sti/pdfs/ADA421056.pdf (02.11.2024)

[3] Ruben Tuitel, *Defining cyberterrorism*, "PerConcordia. Journal of European Security and Defense Issues", Vol. 7, No. 2, 2016, p. 12, https://perconcordiam.com/perCon_V7N2_ENG.pdf (02.11.2024)

[4] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation*, New York, 2015, p. 25

[5] Gabriel Weimann, *Cyberterrorism: How Real Is the Threat? Special Report 119*, United States Institute of Peace, Washington, DC, 2004, https://www.usip.org/sites/default/files/sr119.pdf (02.11.2024)

[6] Uchenna Jerome Orji, *Deterring cyberterrorism in the global information society: A case for the collective responsibility of states*, "Defense Against Terrorism Review", Ankara, Vol. 6, No. 1, 2014, p. 33

Orji's definition highlights cyberterrorism as a specific form of terrorism aimed at critical infrastructures to create threats, destabilization, and panic. Thus, cyber-terrorist actions take on a distinctly political orientation, emphasizing not only the technical but also the strategic level of impact. Orji's approach emphasizes the flexibility that digital space provides to terrorists seeking to influence government decisions and public sentiment.

The Congressional Research Service of the United States has formulated two main approaches to understanding cyberterrorism:

1. Effect-based approach: Cyberterrorism can be defined as computer-based attacks that generate a level of fear comparable to traditional acts of terrorism, even if these attacks are carried out not by terrorists but by criminals.

2. Intent-based approach: Cyberterrorism is defined as an illegal, politically motivated computer attack intended to intimidate or coerce the government or citizens to achieve further political objectives or to inflict significant damage or serious economic harm[1].

According to the researcher at the Institute of Security and Global Affairs at Leiden University T. Tropina, cyberterrorism aims to intimidate the civilian population and government authorities to achieve criminal objectives. She notes that this manifests through threats of violence, the maintenance of a constant state of fear, coercion into specific actions, and drawing attention to the identity of the cyberterrorist or the organization they represent. We support this perspective, as it highlights the unique transparency of cyberterrorism: cyberattacks are often accompanied by public demands, distinguishing them from other forms of cybercrime[2].

One of the earliest legally established definitions of cyberterrorism is found in the "USA Patriot Act of 2001", enacted by the U.S. Congress following the terrorist attacks of 2001. The concept of "cyberterrorism" in this act includes various qualified forms of hacking and damage to protected computer networks belonging to civilians, legal entities, and government agencies, including harm inflicted on computer systems used by government institutions for organizing national defense or ensuring national security[3]. Later, the issue of countering threats in cyberspace increasingly attracted the attention of the global community.

The United Nations document defines cyberterrorism as the use of information and communication technologies (ICT) to execute terrorist acts, including spreading propaganda, recruitment and radicalization, coordinating attacks, and financing terrorist activities. Additionally, cyberterrorism encompasses targeting critical infrastructure, potentially leading to severe economic, social, and physical repercussions. The document highlights the importance of international collaboration and information exchange to counteract cyber threats and secure cyberspace from terrorist activities. This characterization aligns with current challenges, as terrorist exploitation of the internet complicates monitoring efforts and necessitates new measures to control and protect critical information systems at both national and global levels[4].

An analysis of various definitions of cyberterrorism shows that its primary distinction from other types of crimes lies in its goals, which are akin to those of traditional political terrorism—intimidating or coercing governments or populations into specific political or social actions. In this context, attacks using information technology must result in harm to individuals or significant

[1] Prem Mahadevan, *Cybercrime. Threats during the COVID— 2019 Pandemic,* Global Initiative Against Transnational Organized Crime, April 2020, https://globalinitiative.net/wp-content/uplApril020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf (02.11.2024)

[2] Tat'yana Tropina, *Kiberprestupnost'. Ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: monografiya*, Vladivostok, 2009, p. 237

[3] United States Congress, *USA Patriot Act of 2001*, congress.gov/107/plaws/publ56/PLAW-107publ56.htm (02.11.2024)

[4] United Nations Office on Drugs and Crimes, *The Use of the Internet for Terrorist Purposes,* New York, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (02.11.2024)

property damage. Thus, cyberterrorism can be characterized by several key features: the use of technology for attacks, political motivation of the attackers, and the infliction of substantial harm on citizens, organizations, or states.

Features of cyberterrorism as a new kind of terrorist attacks

A cyberattack is a serious threat to humanity, comparable to nuclear, biological, and chemical weapons. Due to its novelty, the extent of this threat is not yet fully recognized or studied. A cyberattack knows no national borders, and a cyberterrorist can equally threaten information systems located almost anywhere on the globe. Detecting and neutralizing a virtual terrorist is extremely challenging due to the minimal traces they leave behind and the unique virtual nature of these traces[1].

Some researchers identify various methods for conducting cyberattacks, including unauthorized access to classified government and military data, banking information, and personal data; causing damage to elements of cyberspace, such as disrupting power grids, creating interference, or introducing viruses to destroy hardware; theft, damage, or destruction of critical information and software through hacking and spreading viruses; disclosure and blackmail through the publication of confidential information; taking control of secured media channels to spread disinformation, demonstrate terrorist strength, or issue demands; and destruction or manipulation of communication lines. A critical concern is the vulnerability of essential infrastructure systems—such as transportation, nuclear power plants, water supply, and energy networks—that are increasingly connected to the Internet[2].

Cyberterrorism should include attempts to disrupt or destroy the functioning of computer systems or the information infrastructure networks of the state or governing bodies. Such criminal acts targeting critical information infrastructure represent a significant threat that could have the most serious consequences for society.

The Maryville University classifies cyberterrorism attacks into three main categories:

Malware: Malicious software refers to programs designed to infiltrate computers and networks without permission, causing damage or disruption with the intent to harm the victim or generate financial profit for the attacker. Common methods for delivering malware include phishing emails, email attachments, harmful advertisements, fake software installation files, and infected USB drives or applications. Various types of malwares include ransomware, which locks or encrypts data for ransom, viruses that trigger harmful actions upon activation, worms that replicate across systems, and spyware that monitors user activity, captures communications, and collects personal information.

Phishing: An attack disguised as an email is designed to deceive the recipient into executing malware that gathers personal data or causes other types of harm. This method is widely used by cyber terrorists and criminals to compromise the devices and networks of their targets. A growing trend in cybercrime involves attackers concentrating on developing the ransomware payload while outsourcing the phishing aspect to a third party, known as an "initial access broker".

Ransomware: Malicious software that locks the victim out of their computer files and restricts access to other resources, only releasing them once a ransom is paid, typically in cryptocurrency like Bitcoin. Ransomware is commonly spread through phishing attacks or more advanced spear phishing

[1] Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?* Special Report 119, United States Institute of Peace, Washington, DC, 2004, pp. 2-3, https://www.usip.org/sites/default/files/sr119.pdf (02.11.2024)

[2] Li Yuchong, Liu Qinghui, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, "Energy Reports", Vol. 7, 2021, p. 8177, https://www.sciencedirect.com/science/article/pii/S2352484721007289 (02.12.2024)

attempts, which rely on social engineering tactics to deceive the victim into opening the file and triggering the attack[1].

The development of technological tools in the era of the information society has created new opportunities for cyberterrorist activities, such as identity theft and impersonation, sensitive data breaches for malinformation purposes or shutting down national official information outlets to sow public discord and mistrust in authorities. These new developments of the digital society significantly impact the security of the state. The active use of the Internet and information technologies by various terrorist organizations is one of the new dangerous threats to the global community. In the context of the information society, cyberterrorism has become a significant threat that actively uses the Internet and digital technologies to achieve terrorist goals. Among the main aspects are coordination of actions, information gathering, fundraising, psychological influence, and recruitment of accomplices. The Internet provides terrorist groups with the opportunity to organize operations, reach a broad audience, and even disseminate instructions for creating explosives. As a result, cyberterrorism creates new challenges for state and international security, requiring enhanced coordination to counter this threat.

Conclusions

In the 21st century, cyberterrorism has become a distinct and increasingly prevalent form of terrorism, presenting amplified risks amid widespread digital interconnectivity and limited regulatory oversight. Combating cyberterrorism effectively requires a multi-layered strategy, involving in-depth research, collaboration between governmental bodies and civil organizations, early detection mechanisms, legal framework enhancements, and robust preventive measures. Such a comprehensive approach is essential to minimize vulnerabilities and enhance resilience against cyberterrorist activities on both national and global scales.

The danger of cyberattacks with a terrorist intent or orientation lies not only in the potential for causing significant harm to a large, indeterminate number of individuals but also in the vulnerability of cyberspace to such attacks or terrorist acts and the likelihood of causing enormous material damage. A distinctive feature of terrorist operations is that achieving these objectives does not require substantial investments. From a cost-benefit perspective, cyberspace becomes extremely attractive to terrorists.

Another aspect that deserves attention is the development and evolution of artificial intelligence. We believe that the question of whether the possibilities and opportunities provided by AI will be exploited for malicious purposes is merely a matter of time.

Given the rapid evolution of cyber tactics and geopolitical tensions, future research should also focus on developing proactive countermeasures, analyzing the motivations and tools employed by cyberterrorists, and anticipating potential vulnerabilities within digital infrastructures. As the cyber landscape continues to shift, the alignment of global policy and defense efforts will be crucial in sustaining long-term resilience against cyberterrorism. The ongoing information warfare that underpins current geopolitical conflicts underscores the urgency of these efforts, suggesting that cyberterrorism will likely intensify as a key security challenge in the years ahead.

Bibliography

Books

[1] Maryville University, *Cyber Terrorism: What It Is and How It's Evolved*, https://online.maryville.edu/blog/cyber-terrorism/#examples (26.11.2024)

1. Tropina, Tat'yana, *Kiberprestupnost'. Ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: monografiya*, Vladivostok, 2009
2. Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation*, New York, 2015

Studies and Articles

1. Barry, Collin, *The Future of Cyber Terrorism*, "Crime & Justice International", Vol. 13, No. 2, March 1997
2. Che, Eliot, *Securing a Network Society: Cyber-Terrorism, International Cooperation, and Transnational Surveillance, Research Paper No. 113, Research Institute for European and American Studies (RIEAS*), Athens, September 2007, https://rieas.gr/images/RIEAS113ELIOTCHE.pdf
3. Denning, Dorothy E., *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representative*s, May 23, 2000, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm
4. Denning, Dorothy E., *Is Cyber Terror Next?*, "Social Science Research Council", https://items.ssrc.org/after-september-11/is-cyber-terror-next/
5. Ebner, Nick, *Cyber Space, Cyber Attack and Cyber Weapons A Contribution to the Terminology*, "Institute for Peace Research and Security Policy at the University of Hamburg", Hamburg, October 2015, https://epub.sub.uni-hamburg.de/epub/volltexte/2018/80797/pdf/IFAR2_ FactSheet7.pdf
6. Ejova, Cristina, *Unele abordări conceptuale ale terorismului*, "Studia Universitatis Moldaviae. Științe Sociale", No. 3, 2023, https://social.studiamsu.md/wp-content/uploads/2023/05/31_C_Ejova.pdf
7. Hirschmann, Kai, *The Changing Face of Terrorism*, "International Politics", No. 3, 2000, https://library.fes.de/pdf-files/ipg/ipg-2000-3/arthirschmann.pdf
8. Li, Yuchong; Liu, Qinghui, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, "Energy Reports", Vol. 7, 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289
9. Mahadevan, Prem, *Cybercrime. Threats during the COVID-19 Pandemic*, Global Initiative Against Transnational Organized Crime, April 2020, https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf
10. Orji, Uchenna, Jerome, *Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States*, "Defense Against Terrorism Review", Vol. 6, No. 1, 2014
11. Pollitt, Mark, M., *Cyberterrorism: Fact or Fancy?*, "Computer Fraud and Security", February 1998
12. Tropina, Tat'yana, *Kiberprestupnost' i kiberterrorizm: pogovorim o ponyatijnom apparate*, in *Informacionnye tekhnologii i bezopasnost. Sbornik nauchnyh trudov mezhdunarodnoj konferencii, Nacional'naya akademiya nauk Ukrainy*, Kyiv, 2003
13. Tuitel, Ruben, *Defining Cyberterrorism*, "PerConcordia: Journal of European Security and Defense Issues", Vol. 7, No. 2, 2016, https://perconcordiam.com/perCon_V7N2_ENG.pdf
14. Weimann, Gabriel, *Cyberterrorism: How Real Is the Threat?*, Special Report 119, United States Institute of Peace, Washington, DC, 2004, https://www.usip.org/sites/default/files/sr119.pdf
15. Wilson, Clay, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues*, October 2003, https://apps.dtic.mil/sti/pdfs/ADA421056.pdf

Documents

1. Center for Strategic and International Studies, *Significant Cyber Incidents*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
2. Check Point, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks*, July 2024, https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/
3. Digital 2024: Global Overview Report. https://indd.adobe.com/view/8892459e-f0f4-4cfd-bf47-f5da5728a5b5
4. Maryville University, *Cyber Terrorism: What It Is and How It's Evolved*, https://online.maryville.edu/blog/cyber-terrorism/#examples

5. UN General Assembly, *Resolution A/54/49: Developments in the Field of Information and Telecommunications in the Context of International Security*, December 1, 1999, https://documents.un.org/doc/undoc/gen/n99/777/13/pdf/n9977713.pdf
6. United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
7. United States Congress, *USA Patriot Act of 2001*, congress.gov/107/plaws/publ56/PLAW-107publ56.htm

Websites

1. https://blog.checkpoint.com/
2. https://www.congress.gov/
3. https://www.csis.org/
4. https://www.unodc.org/
5. https://www.usip.org/

Claudia-Alecsandra GABRIAN
Babeș-Bolyai University, Romania

RANSOMWARE IN THE AGE OF AI: NAVIGATING CYBERSECURITY CHALLENGES IN HYBRID WARFARE

Abstract:	*While the volume of ransomware threats continues to escalate around the world, AI revolutionizes the landscape of cyber offense and defense. Ransomware now evolves into an even more flexible and complex weapon, enabled through AI, morphing into a tool to attack critical infrastructure by state-sponsored opponents. Attackers leverage automation, adaptive encryption, and advanced phishing, whereas defenders employ AI-driven predictive algorithms, behavioral analysis capabilities, and real-time anomaly detection. On the one hand, AI for defense is limited by the vulnerability to adversarial attacks and rapid evolution of malware-both very serious challenges.* *The case studies will present the ransomware's role in hybrid warfare heighten national security risks and geopolitics. Argument: AI has transformed ransomware from a simple form of cyber extortion into an effective weapon for destabilizing the key infrastructures of a nation. Why it matters: Resilient knowledge of this evolution will be the knowledge that is needed for developing resilient cybersecurity strategies. Main question: What constitutes ransomware as a feasible hybrid tool of war? Objective: Identify and evaluate the challenges AI-driven ransomware presents for cybersecurity in hybrid warfare. Literature Review: A review of recent studies on the application of AI within the context of ransomware and hybrid warfare, reports on ransomware attacks and groups of cybercriminals. Data Analysis: Reviewed trends in the evolution of ransomware, AI development, and hybrid warfare strategies.*
Keywords:	**Cybercriminal groups; ransomware; artificial intelligence; critical infrastructure; AI tools**
Contact details of the authors:	E-mail: claudia.gabrian@ubbcluj.ro
Institutional affiliation of the authors:	**Babeș-Bolyai University, Doctoral School of International Relations and Security Studies**
Institutions address:	Mihail Kogalniceanu, no. 1 Street 400084, Cluj-Napoca, România; Tel: +40 264 405 300; Fax: +40 264 591 906, https://www.ubbcluj.ro/en/

Introduction

The nature of conflict, in these times of AI-driven warfare, has grown beyond physical battlegrounds into cyberspace where digital tools along with AI are being used to disrupt, disable, or manipulate adversaries. Hybrid conflicts combine conventional military operations with cyberattacks, disinformation, and economic sabotage. Thus, it becomes a dominant strategy both for state and non-state actors. Hybrid war applies to the use of classic military actions in addition to asymmetric activities, like cyberattacks, to destabilize and destroy a target. Cybermeasures, including ransomware attacks, increasingly form part of this. Most importantly, AI transforms ransomware and other cyber tactics, making such attacks faster, targeted, and adaptable. The new code Rust in russian is the modernization of ransomware-a new challenge to critical infrastructure protection and national security in an AI-driven cyber landscape.

The evolving threat of ransomware is one of the major challenges in this conflict landscape. Ransomware attacks are some of the persistent cybersecurity attacks, where malicious actors encrypt important information until a requested ransom is paid for access. These attacks exploit weaknesses in communication networks and critical infrastructure, and lately, they have been using advanced AI algorithms that help them

identify targets of high-risk systems. In AI-powered ransomware campaigns, automation in scaling phishing attacks, optimization in malware delivery, and evasion of traditional cybersecurity defenses are realized.

Ransomware now can be used in hybrid warfare to disrupt societies and critical sectors, such as healthcare, finance, and government. Leveraging AI, an adversary could go on to render any ransomware attack more precise, at scale, and with strategic and psychological consequences on both civilian and military targets. Moreover, AI-powered automation allows cybercriminals to orchestrate an attack against global networks faster and on a wider scale. The same multiplies the challenge of cybersecurity defense. The combination of AI-driven warfare and ransomware creates an increasingly dangerous setting in which the security of the world would face a serious threat. As more communications technologies are put to military and civilian use, the establishment and enforcement of superior cybersecurity controls become quite vital as a counterbalance to these AI-enabled threats. It would have to involve reaping the support of governments, corporations, and international security agencies in developing AI-based defenses against the continuing ransomware threat in hybrid conflict scenarios.

In the literature review, there are a lot of studies that include AI applications in cybersecurity, focusing on both offensive and defensive strategies. Some articles that are relevant to this topic show that using AI, cyberattacks have become increasingly frequent, impactful, and sophisticated. Nowadays, the dual-edged nature of AI is used for the benefit of organizations and cyber criminals, this means that defensive AI uses machine learning (ML) and other AI techniques to improve the security and resilience of computer systems and networks against cyber-attacks. Conversely, offensive AI takes advantage of the abuse of AI for malicious activities. Some examples include creating new cyberattacks or automating the exploitation of existing vulnerabilities. Also, a third part is correlated with adversarial AI or abuse of AI systems. That can be defined as attacks that might exploit vulnerabilities in AI systems to cause them to make incorrect predictions with either manipulation over the input data feeds to the AI system or poisoning up the training data on which the respective AI system was trained[1].

In support of such expert analysis, many forms of cyber defense systems have been designed in support and collaboration with experts. This is important in ensuring privacy and the integrity of information are secure and accessible through cybersecurity systems from internal and external threats. Therefore, the general purpose of cybersecurity systems is to combat security threats emanating from online sources, even including ransomware. Consequently, there has been a need for the more dependable cybersecurity infrastructure that encompasses both the defensive and offensive approaches through the employment of advanced methods for the discovery of previously unknown cyber intrusions and techniques. In general, defensive approaches use reactive strategies that are focused on prevention, detection, and responses. This is the more a traditional method to keep networks safe from the cybercriminal and requires a thorough understanding of the system to be secured. Understanding of the system and various weak points gives rise to the development of preventive measures. The offensive approaches, on the other hand, are a counterpoint to the defensive methods and proactively predict and remove threats in the system using various ethical hacking techniques. As a vast volume of data is accessible and cyber criminals attempt to get illegal access to cyber-infrastructures, various techniques of Artificial Intelligence and Machine Learning have been explored. This is because ML-based cybersecurity solutions, both offensive and defensive, have been able to handle and analyze large volumes of data and complex detection logic that were tough to handle using traditional methods[2].

One important and dynamic theme that this article shows within the transformative potential of AI in countering emerging cyber threats is the adaptability of defense strategies set within cybersecurity. The key to this adaptability is AI-driven models, which are able to learn dynamically and change in real-time. This responsiveness is so important given that cybercriminal actors have adapted their strategies on a moment-by-moment basis to affect their attack. Having a background in machine learning algorithms and pattern recognition, Artificial Intelligence can check new attack patterns rather swiftly that could be evading conventional static defenses. This is the ability that will let cybersecurity professionals stay ahead of the

[1] Masike Malatji, Alaa Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, Springer, February 2024, https://link.springer.com/article/10.1007/s43681-024-00427-4#citeas (23.11.2024)

[2] Jennifer Tang, Tiffany Saade, Steve Kelly**,** *The Implications of Artificial Intelligence in Cybersecurity*, Virtual Library Reports, October 2024, https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/ (23.11.2024)

evolving threats and provide rapid development of countermeasures. The situational awareness gained allows for quicker, more informed decisions to be made, thus enabling pro-active responses to take place on all kinds of possible threats. Basically, it implies a complete paradigm shift in cybersecurity-that adaptability is now extended to AI-powered defense strategies. It does this by incorporating machine learning on top of dynamic threat modeling, thus going beyond rule-based traditional approaches. This ensures powerful defense that can rapidly counter and neutralize newly emerging cyber threats in today's rapidly shifting digital landscape[1].

The most notorious use of AI is the negative use of the technology by malicious actors for harm against the automated industry with the very methods that were designed for protecting the system. Being modular, AI can be shaped for threat and destruction rather than just safety and reliability. Besides, the vulnerabilities in the AI methods raise much more security concerns and threaten exploitation where attackers can manipulate the algorithms, invoke unnormal behaviors in the mechanism, and launch attacks such as adversarial attacks. The cyber criminals often divert the legitimacy of AI for this purpose to gain some personal benefits. AI incorporated attacks can be challenging to the security of the system as it can adapt to the security measures to evade detection, prevention, and mitigation techniques[2].

Defining ransomware and hybrid warfare

The typical lifecycle that defines ransomware includes infiltration, encryption, a demand for ransom, and possible decryption or destruction of data. Initially, ransomware was more opportunistic, often affecting individuals and small businesses. However, it has grown into a sophisticated tool that is well used against large organizations and vital infrastructures, causing unparalleled disruption. The evolution has further led to even more sophisticated versions like Ransomware-as-a-Service that allows even none-tech-savvy cybercriminals to conduct ransomware attacks[3].

Hybrid warfare integrates all these traditional military objectives with cyber, information, and psychological operations directed at an enemy to force strategic accomplishment of goals without resorting to conventional fighting. The form of war would also include the use of cyberattacks, such as ransomware, to disrupt basic services, create socioeconomic turmoil, and even further weaken the economy of an adversary. As such, where cyber capabilities have been used for the defeat of essential infrastructure as part of hybrid war techniques, state and state-sponsor actors are able to influence pressure in politically sensitive regions without necessarily resorting to conflict. When it strikes vital services in energy, health, and others, ransomware can be included as part of hybrid warfare, acting as a geopolitical instrument of influence and coercion[4].

AI is playing a increasingly bigger role in ransomware, amplifying their effectiveness, adaptability, and stealth. Attackers use AI-powered techniques to automate ransomware delivery, enhance social engineering, and evade detection-all factors that complicate defense efforts. In the context of hybrid warfare, AI-enhanced ransomware is a low-cost, high-impact tool that state-sponsored actors can use to disrupt essential services relatively anonymously. Since AI enables adaptable and evasive attacks, it will be more challenging to identify the origin of ransomware as coming from a particular group or nation, making diplomatic responses difficult and adding additional complications to national security. Tools that are used:

Automation of Ransomware Delivery and Execution: AI algorithms are making it easier to deploy ransomware across a large network because they can automate the tasks involved in deploying ransomware, such as scanning for vulnerabilities, moving laterally within a network, and encrypting files, as has been seen in attacks like WannaCry and NotPetya.

Advanced Social Engineering Techniques: Using machine learning algorithms that analyze current social media information, patterns in people's email use, and other public information, highly convincing

[1]Badria Sulaiman Alfurhood, Dattatreya Mankame, Meenakshi Dwivedi, *Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies*, https://www.researchgate.net/publication/376375202_Artificial_Intelligence_and_Cybersecurity_Innovations_Threats_and_Defense_Strategies (23.11.2024)

[2]Rafy Fazley, *Artificial Intelligence in Cyber Security*, https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security (23.11.2024)

[3]Cybersecurity and Infrastructure Security Agency (CISA)**,** *Ransomware Guide*, Stop Ransomware, https://www.cisa.gov/stopransomware/ransomware-guide (01.11.2024)

[4]Broadcom, *Symantec Internet Security Threat Report*, Symantec, Vol. 3, January 2023, https://docs.broadcom.com/doc/istr-03-jan-en (01.11.2024)

phishing messages can be built targeted against a specific individual or organization; Adaptation to Detection and Evasion: Most of the traditional cybersecurity tools use known patterns or signature-based detection of malware for their detection. Artificial intelligence uses deep learning and machine learning models and enables ransomware to evade these defenses by adapting in real time[1].

Analyzing reports on ransomware attacks shows that ransomware is considered one of the most widespread attack vectors in the modern world, also through the Ransomware-as-a-service model. The ransomware ecosystem has visibly evolved during the first half of 2024, were notable changes in the methodologies of attack, victimology, and tactics of cybercriminals. The team from Rapid7 identified 21 new ransomware groups coming onto the scene in the first six months of 2024, some of them are brand new, while others have been rebranded as previously known groups.

The use of encryption algorithms such as AES, RC4, and especially ChaCha underlines a strategic decision taken by ransomware groups to optimize performance and security evasion. Such evolution of infection techniques is part of the more general trend for cybercriminals to focus on increasingly sophisticated tools and upgrading the effectiveness of their attacks.[2] Also, is important to analyze the next six months for 2024, to see if these cybercriminal groups can reestablish and adapt their techniques to launch cyberattacks using AI methods.

The evolution of ransomware with AI capabilities

Ransomware attacks moved during the 2010s from targeting individual users to big organizations and critical infrastructures. Although RaaS platforms had given an opportunity for less technical criminals to commit such attacks, a series of highly visible ransomware attacks, such as WannaCry and NotPetya, showed how much disruption ransomware could cause. Further, throughout the 2020s, artificial intelligence accelerated this evolution by making ransomware a lot more automated, adaptive, and persistent[3]. AI technologies transformed ransomware into a more sophisticated, evasive, and effective weapon. The main AI-powered improvements include:

Automation and Scaling: AI makes it possible for ransomware attackers to automate every step of the attack, from initial compromise all the way to lateral movement. AI-driven automated tools can identify and exploit weaknesses much faster and at higher scales than would be possible manually. Attackers use machine learning in refining their targeting precision by selecting victims based on industry, network vulnerability, or payment potential that improves the overall success rate of ransomware[4].

Adaptive Encryption and Behavior: Traditional ransomware encrypted files in a predictable and, therefore, detectable pattern. AI makes it possible for ransomware to adapt to various encryption algorithms, changing dynamic behavior and becoming more evasive to traditional static defense mechanisms. The adaptive encryption allows ransomware to selectively encrypt important files, many times waiting to evade initial scans before launching a full attack-a ploy that gives attackers an upper hand over traditional detection models which might not identify altered encryption patterns[5]. Advanced Social Engineering/Phishing Techniques: Traditionally, phishing has always been one of the popular delivery methods of ransomware, but it is now

---

[1] Gavin Hull**,** John Henna, Arief Budi, *How to improve cybercrime investigations: A review of the digital forensic literature in the wake of recent technological advancements*, "Crime Science", Vol. 8, No. 9, September 2019, https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0097-9 (01.11.2024)

[2] Rapid7, *2024 Ransomware Radar Report*, October 2024, https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf (23.11.2024)

[3] CSO, *A history of ransomware: The motives and methods behind these evolving attacks*, July 2020, https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html (01.11.2024)

[4] Benjamin Jensen, Yasir Atalan, Jose Macias, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence (01.11.2024)

[5]Microsoft Corporation, *Microsoft Digital Defense Report 2024*, Microsoft Security Insider, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (01.11.2024)

more effective because of AI. Through machine learning algorithms, it can analyze an enormous amount of data with the ability to create highly personalized phishing emails around possible targets[1].

AI-Driven capabilities enhancing ransomware in hybrid warfare

Hybrid warfare will continue to evolve with advances in technology and will shift the geopolitical environment. In as much as state and non-state actors will continue to leverage cyber-capabilities in the immediate future, the integration of digital warfare is very much a cornerstone of hybrid strategies. This evolution increases the complexity of conflict and further blurs the lines between traditional and unconventional military engagements[2].

For instance, emerging technologies using artificial intelligence will accelerate the speed of decisions and increase the accuracy of operations. They will advance intelligence collection and disrupt adversary communications, underlining the need for agile and creative countermeasures. Automation of ransomware in hybrid warfare enables state-sponsored groups to conduct large-scale attacks with unprecedented velocity and accuracy, often overwhelming traditional defenses. They can strike many critical systems, crippling energy, transportation, and healthcare sectors with more operations. AI-driven adaptive encryption increases the evasive capabilities of ransomware. While older ransomware relies on static encryption methods, AI-enhanced ransomware can dynamically switch to different keys or algorithms to thwart decryption or forensic analysis. Adaptive encryption provides the ransomware with the intelligence to adaptively adjust to the specific defensive layouts of a target-such as switching to a different encryption algorithm if the previous one was detected as vulnerable, thereby keeping the data locked. Ransomware can be adaptive in that it changes its code to evade traditional antivirus detection, especially with polymorphic ransomware. In hybrid warfare, adaptive encryption can be strategically targeted at critical infrastructure, with data recovery, being difficult, especially for high-value targets such as government agencies and defense organizations[3].

One of the most potent contributions AI has made to ransomware is its capability for personalized attack through custom targeting. The attackers will apply machine learning algorithms to aggregate multiple volumes of data on individuals and organizations, tailoring the methods of delivery for the ransomware in hopes of increasing the potential success rate of an attack. Examples involve AI-powered tools that monitor communication patterns of a target, their social media usage, and network activity; this provides insight into the ways to infiltrate the network most effectively through things like highly customized phishing emails or crafted malware downloads[4].

In hybrid warfare, ransomware strikes, tailored for specific targets, are allowed on selected victims by state-sponsored actors based on their political, economic, or military importance. Examples target critical infrastructure, such as power grids and telecommunications systems, to create maximum disruption. Furthermore, malware can also be tailored for specific languages, cultures, and sectors, which will make sure that the ransomware really resonates and spreads effectively in the targeted environment. The evasiveness of ransomware during the compromise of critical systems for extended durations presents difficult countermeasures, particularly in high-value environments such as defense networks, government agencies, and financial institutions[5]. AI greatly enhances the efficiency of spear-phishing and social engineering tactics, which usually serve as entry points for ransomware. Conventional phishing emails have generic messages and broad targeting, hence being much easier to identify as suspicion prone. With AI, immense personal and organizational data can be analyzed to send tailor-fit phishing emails that look quite legitimate. Machine

[1] CrowdStrike, *Types of Social Engineering Attacks*, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ (01.11.2024)

[2] Total Military Insight, *Historical Examples of Hybrid Warfare*, July 2024, https://totalmilitaryinsight.com/historical-examples-of-hybrid-warfare/ (23.11.2024)

[3] SentinelOne, *What is Polymorphic Malware?*, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/ (02.11.2024)

[4] Microsoft Corporation, *Audience Targeting*, https://about.ads.microsoft.com/en/tools/performance/audience-targeting (02.11.2024)

[5] Frank Hoffman, Matt Neumeyer, Benjamin Jensen, *The Future of Hybrid Warfare*, Center for Strategic and International Studies, July 2024, https://www.csis.org/analysis/future-hybrid-warfare (02.11.2024)

learning algorithms will tune messages based on a target's recently observed social media activity and professional contacts[1].

AI-Driven defense mechanisms against ransomware

AI-powered predictive models are changing the face of ransomware defense through swift identification of precursors to potential threats before they enter a system. Predictive models, by analyzing big data sets inclusive of attack patterns, vulnerabilities, and system configurations, compute the environments that are at greater risk and predict when and where the ransomware attacks will take place. AI-powered threat intelligence solutions aggregate feeds in real time, analyze the information, and present insights to the security teams for timely awareness of the latest emerging threats and how ransomware patterns are trending. Most of them are designed on machine learning models that have been trained on previous attacks and computer signals to identify early warning signals that will enable the organization to patch the vulnerabilities as well as change firewall settings, among other preventive measures, to avoid infiltration[2].

Predictive algorithms represent early warnings of highly organized ransomware campaigns in hybrid contexts of war, allowing governments and critical sectors to prepare their defenses in anticipation of possible state-orchestrated cyberattacks. This is of great essence in securing critical infrastructure, where the stakes for a ransomware breach could be as high as national security and public safety[3]. This would be the most important capability in a hybrid war scenario to strike back ransomware against critical infrastructure, as behavioral analysis tools can detect and mitigate ransomware threats aimed at basic infrastructure-like power grids, healthcare, and communications systems of any type in a way that would really lessen possible disruption[4].

Anomaly Detection Systems have improved response times by real-time alerts to security teams, the automatic responses include system isolation and blocking suspicious traffic. AI is not only helpful at the stage of detecting ransomware but also in coordinating rapid response and recovery. AI-driven automated incident response systems can triage security alerts, prioritize incidents down to those that need attention, and can even take containment steps such as disconnecting the affected device from the network[5]. AI can further reinforce such recovery efforts by locating and restoring critical files from backups and isolating encrypted files to stop further proliferation[6]. AI is changing the face of ransomware defense by having predictive, responsive, and adaptive capabilities that normally are not achievable with conventional cybersecurity means. Tools of modern AI-driven ransomware defense include:

Predictive algorithms: These algorithms analyze past ransomware attack data for patterns that can help in predicting future threats. Such algorithms evaluate the extra vulnerabilities an attack may cause in a network and provide proactive defense mechanisms to cybersecurity teams, which would alert them about areas of high risks or recommend proactive defenses.[7]; Behavioral Analysis and Anomaly Detection: AI-driven behavioral analytics solutions identify patterns of activity operating out of the ordinary, which, in this context, could mean an imminent ransomware attack. Anomaly detection provides additional security in that it will include all those minor and minute variations that perhaps the static defense mechanisms would not be able to detect[8].

The qualitative analysis revealed that to assess the effectiveness of AI-driven defense mechanisms is important to develop robust intrusion detection systems for cyberthreats, such as ransomware, because is important to understand malware behavior. Machine learning stands at the forefront of automating behavior

[1] Trend Micro, *Spear Phishing*, http://www.trendmicro.com/vinfo/us/security/definition/spear-phishing (02.11.2024)

[2]World Economic Forum, *AI and Cybersecurity: How to Navigate the Risks and Opportunities*, https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/ (02.11.2024)

[3]Microsoft Corporation, *What is Behavioral Analytics?*, https://www.microsoft.com/en-us/dynamics-365/topics/ai/customer-insights/what-is-behavioral-analytics, (02.11.2024)

[4] Fortinet, *Network Traffic*, https://www.fortinet.com/resources/cyberglossary/network-traffic (02.11.2024)

[5]Broadcom, *Symantec Ransomware Threat Landscape 2024*, https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf?hsCtaTracking=767be7a3-c8a1-4cd1-8387-7ec8ac770b3c|e27274de-c76f-4496-ac64-e943054afaa8 (02.11.2024)

[6] IBM, *AI Cybersecurity*, https://www.ibm.com/ai-cybersecurity (02.11.2024)

[7] IBM, *Predictive Analytics*, https://www.ibm.com/topics/predictive-analytics (02.11.2024)

[8]CrowdStrike, *AI-Powered Behavioral Analysis*, https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/ (02.11.2024)

analysis through informative feature extraction from network packets and paving the way for developing sophisticated intrusion detection systems. Deep learning (DL) defense mechanisms are increasingly deployed to automate the identification of cyber threats and with these systems continuously evolving can enhance effectiveness over time. The primary themes are related to regular updates for DL to maintain effectiveness[1], and various mitigation strategies against different types of AI-driven cyberattacks for empirically assessing effectiveness.

AI-empowered and real-time network traffic analysis extends aptitudes for more detection and neutralize potential threats. Furthermore, AI-powered threat intelligence uses global threat landscapes and historical data to predict and to respond proactively to new threats. Automation is one of the most important aspects of artificial intelligence in the process of threat mitigation through the coordination of responses. By putting threat data in context and discerning the real from the false, context-aware AI systems reduce the chance of missing a security incident and [2]AI-based models can repair cybersecurity bugs in a code[3].

AI technology integrated with human expertise in cybersecurity improves the efficiency of threat detection mechanisms. Conclusively, AI technology has revolutionized cybersecurity incident response by introducing automation that augments efficiency and effectiveness within cybersecurity defense strategies respecting threat detection and mitigation.[4] AI models will learn a pattern and behaviors found in previously collected data; this is potentially less effective in malware detection for sophisticated ransomware operating. This reliance on historical data creates a blind spot concerning zero-day ransomware attacks-new subtypes that take advantage of unknown security vulnerabilities[5].

Case studies

In 2017, ransomware attack known as WannaCry used exploits against unpatched systems to rapidly spread across networks. Whereas during the time this attack occurred, several organizations' defenses were using AI-based defenses, none of these systems identified the propagation strategy used by WannaCry-a limitation pointing to a gap in training AI models on pre-existing attack behaviors. The inability to detect WannaCry, in this respect, underlines fully the risks of relying solely on machine learning models that cannot adapt to new, previously unknown forms of attack. This incident, thus, puts into focus the importance of having updated patches along with system defenses in addition to the solutions provided by AI[6].

As a short analysis, WannaCry, sometimes also called WCry or WanaCryptor was a ransomware malware. The virus that was associated with ransomware had worm functionality since it is able to spread itself within infected networks. Following the completion of encryption, a ransom note was displayed to the user, in which the attackers ask for $300 to be paid in a 3-day time span. The ransom amount increases to $600 if the victim resists, which is to be paid in 7 days. In that attack in 2017, an EternalBlue exploit was used, believed to have been developed by the American NSA and which had previously been leaked by a cybergang known under the alias “The Shadow Brokers”. This exploit affects the Windows operating system, for which the company provided a patch to fix in a rush. Unfortunately, many individuals and organizations that did not update computers were targeted in this attack, more than 200,000 computers worldwide were infected with WannaCry within a few days when the attack. A fix of the EternalBlue exploit, along with finding the “kill switch” that allowed stopping the execution of the malware, were the two main contributions helpful in

[1] Aya Salem, Saffa Azzam, *Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques*, “Journal of Big Data”, Vol. 11, No. 105, August 2024, https://doi.org/10.1186/s40537-024-00957-y (23.11.2024)

[2]Masike Malatji, Alaa Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, “*AI and Ethics”*, February 2024, https://doi.org/10.1007/s43681-024-00427-4 (23.11.2024)

[3]Irshaad Jada, Thembekile Mayayise, *The impact of artificial intelligence on organizational cybersecurity: An outcome of a systematic literature review*, “*Data and Information Management”*, June 2024, https://doi.org/10.1016/j.dim.2023.100063 (23.11.2024)

[4]HacknJill, *Can Cybersecurity Be Replaced by AI?*, https://hacknjill.com/cybersecurity/advanced-cybersecurity/can-cybersecurity-be-replaced-by-ai/ (23.11.2024)

[5] Jannatul Ferdous, et.all., *AI-Based Ransomware Detection: A Comprehensive Review*, “IEEE Xplore”, Vol. 12, September 2024, https://ieeexplore.ieee.org/document/10681072 (03.11.2024

[6] CSO, *WannaCry Explained: A Perfect Ransomware Storm*, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html (03.11.2024)

slowing down this malicious campaign. By the time it was finished, though, total damage had reached into the billions, with victims in over 150 countries having been affected. A campaign of such scale raised international investigation of the highest level aimed to find out who was behind the outbreak and was find out that ransom notes were most likely written by hand, with the writers seemingly fluent in Chinese[1].

The DarkSide Ransomware Attack on Colonial Pipeline 2021 was another ransomware attack, representing one of the more significant ransomware attacks that had been publicly disclosed to take place against critical infrastructure in the U.S. During the attack, while the pipeline's operational technology systems responsible for physically moving the oil were not directly compromised, they shut down 5,550 miles of pipe. After stealing the data, the hackers infected ransomware in the "IT Network" of Colonial Pipeline, which later spread the attack to many work computers necessary for billing and accounting[2].

The Colonial Pipeline company was responsible for nearly half the fuel supply and is one of the most important pipeline operators in the United States. It carries nearly 45% of fuel for the East Coast: gasoline, diesel fuel, heating oil, jet fuel, and of fuel that military forces use. The company suffered so severely after the attack and after that it was declared a state of emergency status in 18 states to aid in the shortages. Five days since the shutdown prompted by the attack, Colonial Pipeline still cannot resume full operations.[3] The attackers had demanded a ransom of almost $5 million from the victim company, that was paid several hours after the attack and data of 99 victim companies has been leaked to the dark web. Colonial Pipeline recovered some data compromised by the attackers. Even after receiving the decrypt or, the pace to restore the systems remained very slow because of the decrypting tool they got from the attackers, and it had to continue using its own backups to restore its systems[4].

The 2017 ransomware attack on WannaCry and the Colonial Pipeline ransomware attack this year present a geopolitical scenario in which cybercriminals mount cyberattacks on critical infrastructures. 'WannaCry' ransomware, attributed to the North Korean group Lazarus, showed the world how ransomware might be used as a state-sponsored tool not only in crippling economies but as geopolitical pressure in targeting global systems for highlighting lapses in international cooperation relative to cybersecurity norms. Carried out by the hacking group DarkSide, the Colonial Pipeline attack became the latest in a string of ransomware attacks, underlining the increased sophistication of RaaS operations that had substantial economic consequences, such as fuel shortages up and down the U.S. East Coast. This also served to raise tensions between the U.S. and Russia, since groups like DarkSide were said to operate within the Russian sphere of influence. In both cases, the vulnerability of critical infrastructure was underlined, raising debate on international cybersecurity structures, public-private collaboration, and the ethics of ransom payments.

Strategic implications for national security and geopolitics

AI-driven ransomware represents a threat to national security, especially when we talk about critical infrastructure systems such as energy, healthcare, and finance. These are important features in the running of society, and any disruption to the same translates into widespread consequences for both public safety and economic stability. Energy or healthcare access can be disrupted when such facilities fall prey to a ransomware attack, thereby putting lives at risk while weakening peoples' confidence in the security that the government provides. Thus, in this sense, the national security influence of ransomware can be best described by the example of the enormous NotPetya attack in 2017 targeting Ukrainian businesses and government institutions and afterwards quickly propagated to important critical world industries: shipping and energy. While this latter attack was ostensibly financially motivated, the geopolitical consequences were extraordinary, where it seriously disrupted the operations of several multinational companies and caused billions of dollars in

[1] *WannaCry Malware Trends*, https://any.run/malware-trends/wannacry (23.11.2024)

[2] TechTarget, *Colonial Pipeline Hack Explained: Everything You Need to Know*, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (03.11.2024)

[3] TrendMicro, *What We Know About Dark Side Ransomware and the US Pipeline Attack*, https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html (23.11.2024)

[4] Kaspersky ICS-CERT, *Dark Chronicles: The Consequences of the Colonial Pipeline Attack*, Kaspersky ICS-CERT Publications, https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/ (23.11.2024)

economic damage. Because of its impact, the incident has been described by some governments as a kind of cyberwar[1].

Ransomware attacks attributed to state-sponsored actors escalate tensions between nations, and even have been known to lead to diplomatic or military action where, the complication for attribution arises when state actors allegedly support or enable ransomware groups to blow up diplomatic impasses: countries might resort to imposing sanctions, restricting trade, and even cyber-retaliation as deterrents. For instance, ransomware operations that were apparently conducted by Russian groups forced many Western nations to impose sanction and diplomatic measures on Russia for quota increases in international cyber relations[2].

Sanctions and countermeasures only play into the increasingly significant role of cyberspace in geopolitical strategy-where ransomware attacks are not only a question of extracting ransom but also tools of economic destabilization and psychological warfare. This makes the AI emergence in ransomware potentially amplify these effects, since machine learning allows for more targeted and efficient attacks, therefore making large-scale disruption even more likely. It is a strategic use of ransomware that shows how international relations debates about norms in cyberspace, accountability, and the threat of retaliation have to balance the option of exacerbating conflicts as a whole[3].

Beyond the economic costs, ransomware attacks affect public trust in institutions' capabilities for securing basic services. This is further complicated with an uptick in AI-driven ransomware, as this malware evolves around classic defenses, raising both frequency and severity. Such an erosion of trust calls for new regulations on cybersecurity from governments, including mandatory reporting requirements for critical infrastructure and an increased regulation of the cybersecurity practices pursued by the private sector. The emergence of ransomware has, hence, given way to the formulation of policies on infrastructural resilience, defensive policy founded on co-operation, and response[4].

The economic consequence of ransomware is severe, from direct costs-like ransom paid and remediation-to indirect costs, including business interruption and supply chain delays, which impose long-term economic burdens. The most important incidents of ransomware have forced governments and businesses to make a very substantial resource investment in recovery efforts, budgetarily straining and compromising public confidence in institutional cybersecurity measures. The Colonial Pipeline incident is a perfect example of such manifestations since it led to fuel shortages in the Southeastern United States, where gasoline prices rose and industries that depended on the transportation of fuel were affected[5].

Conclusions

Started as financially motivated cybercrime, ransomware escalated in a tool of hybrid warfare, threatening critical infrastructure disruption, economic disruption, and geopolitical destabilization by way of state-sponsored ransomware groups. As ransomware has increasingly become intertwined with AI, it has taken on new capabilities, including adaptive encryption, evasive techniques, and targeted delivery.

The most striking, is how ransomware integrating AI raises the scale, speed, and complexity of a threat that was unprecedented in its proposition towards national security, international relations, and economic stability. Understanding these transformations is essential in crafting effective defenses against this persistent threat. The RaaS model will continue to grow, where less sophisticated cybercriminals will utilize extremely powerful ransomware tools, thereby increasing the frequency and severity of the attacks. Nation-states will leverage malware to conduct espionage, sabotage, and even open conflict. Already, cyber weapons can take the lead in future conflicts; attacks against the critical infrastructures are intended to ensure general chaos.

Nations need to emphasize AI-fortified cyber defense and international cooperation. The integration of AI and ML into malware will open the door to new forms of autonomous, adaptive threats. The use of

[1]CloudFlare, *What are Petya and NotPetya*?, https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/ (05.11.2024)

[2] Hansel Mischa, Silomon Jantje, *Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios*, "Journal of Cyber Policy", September 2023, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2357092#abstract (06.11.2024)

[3] *Idem*

[4] *Idem*

[5]The New York Times, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, https://www.nytimes.com/2021/05/12/business/economy/colonial-pipeline-economic-impact.html (06.11.2024)

ransomware by state actors in hybrid war mechanisms underlines an ever-growing element of complexity and geopolitical importance in cyber warfare. Continuous research in the evolving role of AI in cyber war and further collaboration by nations on the legal frameworks. Ransomware tactics are used by state-sponsored hybrid warfare to disrupt critical infrastructure, destabilize nations, and undermine public confidence. Often, these tactics combine ransomware attacks with other forms of cyber aggression in ways that create unique and complex challenges for defending nations and organizations. The dynamically complex nature of ransomware in state-actor hybrid warfare underlines increasingly complex and geopolitically significant methods of cyber war.

In these ways, the attack of critical infrastructure and forms of ransomware are highly sophisticated, allowing state-sponsored actors to achieve goals of strategic disruption with limited attribution. Due to the inherent difficulties in defending against such kinds of attacks-rapid response, complexity, and the fog of misinformation-considerations should also be made for new approaches: cross-border intelligence sharing, AI mechanisms of defense, and unequivocal policies in terms of incident response for critical sectors. Ransomware being used by state actors as part of hybrid warfare represents an emerging layer of complexity and geopolitical relevance for cyber warfare. But ransomware attacks provide a continuously developing menace against national security, economic stability, and international relations when there is hybrid war. AI-driven ransomware becomes even smart, covers traditional defenses, and complicates attribution.

Case studies like the Colonial Pipeline Attack and similar cases and the hypothetical disruption of communication networks powered by AI require urgent calls for cybersecurity strategies. Lessons learnt from incidents highlight the operational importance of following improvement in attributions, AI-enhanced defense mechanisms, zero-trust policies, and public-private partnerships. Because developments regarding ransomware will continue to go forward with proactive international cooperation, defense against the next generation of hybrid warfare threats must be developed. AI-powered security tools add a new level of sophistication to the cyber defense against ransomware by using predictive algorithms, behavior analysis, and anomaly detection in real time. As AI can amazingly improve response times and threat detection rates, it also introduces challenges. For instance, limitations in adaptability and vulnerability to adversarial attacks. On the other hand, AI also poses certain specific significant challenges that balance its effectiveness in ransomware defense, such as limits to adaptability, adversarial AI attacks, and resource demands.

Gaps in current research

Up until this point, little attention has been paid to offensive and defensive AI in research, as most relevant literature remains anchored to the technological dimension of both defensive-adversarial and offensive AI. This underlines the need for more holistic research on AI in cybersecurity, considering non-technical factors that may influence AI-driven threats. Most research reporting on AI-driven attacks focuses on their technical engineering aspects. This gap points to a more holistic approach in carrying out research on the malicious potential of AI and its social impact, with particular emphasis on trying to understand what the current situation is regarding the AI-driven cyberattack landscape, motivation, mitigation strategies, and social impact. Even with lots of research in the application of AI in cybersecurity, there exists an obvious literature gap in terms of the long-term implications of AI-driven defense strategies. There is significant rare in-depth research evidence that has addressed socio-economic, ethical, and legal issues regarding this integration.

The absence of research in the literature underlines the need for a comprehensive investigation that goes beyond the technical effectiveness of AI in cybersecurity, while emphasizing the larger organization and societal ramifications that influence how digital defense mechanisms develop in the future. Research into the application of AI technologies to cybersecurity makes clear a series of challenges and limitations that use of these advanced technologies will need to be considered. In the context of AI driven cybersecurity, adversarial attacks stand out as a major concern. AI systems have vulnerabilities that malicious actors take advantage of in order to abuse them and produce results that are compromised. This underlines the importance it is to have strong security measures in place that can protect these technologies from manipulation by adversaries. There is a limit introduced by using historical data.

While AI systems are great, they excel at recognizing patterns in historical data; they could be challenged to identify previously unseen threats-what are called “zero-day threats” utilized by ransomware cybercriminals. In the dynamic and constantly changing area of cybersecurity, continuous monitoring, evaluation, and enhancement of AI algorithms become critical to maintaining state-of-the-art threat detection.

If AI is to be used to strengthen cybersecurity without sacrificing the robustness and agility of the mechanisms of defense against sophisticated threats, these issues must be resolved.

Future research directions

Asymmetrical development in cyber war has given rise to much more powerful and devastating attacks due to the wide adaptation and employment of AIs in generating and executing zero-day attacks. Key issues identified in AI-driven cybersecurity, so far, are indirect development of malicious AI-based software; the rising need to understand the reasoning behind AI-driven decisions; and dealing with new types of cyber-attacks whose nature may be devious to the AI mechanism. It is a challenge to have a balance in this aspect since transparency, explainability, fairness, and accountability in view mean that AI cyber resilience supported across the domain is one of those major challenges.

The rapid progress of AI reshapes the ransomware threats, mainly within the quite complex framework of hybrid warfare with state and non-state actors combining cyberattacks with the conventional means. Concretely, findings in the current domain of literature can be directed at areas for future research: the ways in which AI is used in the evolution of ransomware tactics into more dynamic and adaptive forms of malware using machine learning algorithms to evade traditional mechanisms of detection. For example, research can be performed to understand how attackers are using AI to optimize ransomware distribution, personalize ransom demands, and automate reconnaissance on targeted systems. Knowing these developments is bound to be crucial in developing countermeasures by using AI in predictive threat analysis, anomaly detection, and real-time response to these increasingly complex cybersecurity ecosystems.

Other studies might investigate how AI can reinforce a set of defensive measures against ransomware in hybrid warfare attacks since, in general, such attacks target technical and psychological vulnerabilities concurrently. Further research could be conducted on how AI-powered threat hunting tools, like neural networks, which utilize patterns indicative of ransomware before it is fully executed, could apply. The effectiveness of combining AI with blockchain technology for secure data backup and immutable logging of incidents should be one of the core research areas, considering resilience against ransomware and ensuring transparency and accountability in hybrid warfare situations.

Bibliography

Studies and Articles

1. Alfurhood, Badria, Sulaiman; Mankame, Dattatreya; Dwivedi, Meenakshi, *Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies*, https://www.researchgate.net/publication/376375202_Artificial_Intelligence_and_Cybersecurity_Innovations_Threats_and_Defense_Strategies
2. Fazley, Rafy, *Artificial Intelligence in Cyber Security*, https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security
3. Ferdous, Jannatul, et.all., *AI-Based Ransomware Detection: A Comprehensive Review*, "IEEE Xplore", Vol. 12, September 2024, https://ieeexplore.ieee.org/document/10681072
4. Hoffman, Frank; Neumeyer, Matt; Jensen, Benjamin, *The Future of Hybrid Warfare*, Center for Strategic and International Studies, July 2024, https://www.csis.org/analysis/future-hybrid-warfare
5. Hull, Gavin; Henna, John; Budi, Arief, *How to improve cybercrime investigations: A review of the digital forensic literature in the wake of recent technological advancements*, "Crime Science", Vol. 8, No. 9, September 2019, https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0097-9
6. Jada, Irshaad; Mayayise, Thembekile, *The impact of artificial intelligence on organizational cybersecurity: An outcome of a systematic literature review*, "Data and Information Management", June 2024, https://doi.org/10.1016/j.dim.2023.100063
7. Jensen, Benjamin; Atalan, Yasir; Macias Jose, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence
8. Jensen, Benjamin; Atalan, Yasir; Macias Jose, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence

9. Malatji, Masike; Tolah, Alaa, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, Springer, February 2024, https://link.springer.com/article/10.1007/s43681-024-00427-4#citeas
10. Masike, Malatji; Alaa, Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, "AI and Ethics", February 2024, https://doi.org/10.1007/s43681-024-00427-4
11. Mischa, Hansel; Jantje, Silomon, *Ransomware as a threat to peace and security: understanding and avoiding political; worst-case scenarios*, "Journal of Cyber Policy", September 2023, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2357092#abstract
12. Salem, Aya Azzam Saffa, *Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques*, "Journal of Big Data", Vol. 11, No. 105, August 2024, https://doi.org/10.1186/s40537-024-00957-y

Documents and reports

1. *2024 Ransomware Radar Report*, October 2024, https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf
2. *AI-Powered Behavioral Analysis*, CrowdStrike Cybersecurity 101, https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/
3. Broadcom, *Symantec Internet Security Threat Report*, "Symantec", Vol. 3, January 2023, https://docs.broadcom.com/doc/istr-03-jan-en
4. Broadcom, *Symantec Ransomware Threat Landscape 2024*, https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf?hsCtaTracking=767be7a3-c8a1-4cd1-8387-7ec8ac770b3c|e27274de-c76f-4496-ac64-e943054afaa8
5. CloudFlare, *What are Petya and Not Petya?*, https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
6. CSO, *A history of ransomware: The motives and methods behind these evolving attacks*, July 2020, https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html
7. CSO, *Wanna Cry Explained: A Perfect Ransomware Storm*, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html
8. Cybersecurity and Infrastructure Security Agency (CISA)**,** *Ransomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide
9. Fortinet, *Network Traffic*, *Fortinet Cyber Glossary*, https://www.fortinet.com/resources/cyberglossary/network-traffic
10. HacknJill, *Can Cybersecurity Be Replaced by AI?*, https://hacknjill.com/cybersecurity/advanced-cybersecurity/can-cybersecurity-be-replaced-by-ai/
11. IBM, *AI Cybersecurity*, https://www.ibm.com/ai-cybersecurity
12. IBM, *Predictive Analytics*, https://www.ibm.com/topics/predictive-analytics
13. Kaspersky ICS-CERT, *Dark Chronicles: The Consequences of the Colonial Pipeline Attack*, https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/
14. Microsoft Corporation, *Audience Targeting*,
15. https://about.ads.microsoft.com/en/tools/performance/audience-targeting
16. Microsoft Corporation, *Microsoft Digital Defense Report 2024*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
17. Microsoft Corporation, *What is Behavioral Analytics?*, https://www.microsoft.com/en-us/dynamics-365/topics/ai/customer-insights/what-is-behavioral-analytics
18. Tang, Jennifer; Saade, Tiffany; Kelly, Steve, *The Implications of Artificial Intelligence in Cybersecurity*, "Virtual Library Reports", October 2024, https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/
19. TechTarget, *Colonial Pipeline Hack Explained: Everything You Need to Know*, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

20. Total Military Insight, *Historical Examples of Hybrid Warfare*, https://totalmilitaryinsight.com/historical-examples-of-hybrid-warfare/
21. Trend Micro, *Spear Phishing*, http://www.trendmicro.com/vinfo/us/security/definition/spear-phishing
22. Trend Micro, *What We Know About DarkSide Ransomware and the US Pipeline Attack*, https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html
23. The New York Times, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, https://www.nytimes.com/2021/05/12/business/economy/colonial-pipeline-economic-impact.html
24. *Types of Social Engineering Attacks*, Cybersecurity 101, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/
25. *Wanna Cry Malware Trends*, https://any.run/malware-trends/wannacry
26. *What is Polymorphic Malware?*, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/
27. World Economic Forum, *AI and Cybersecurity: How to Navigate the Risks and Opportunities*, https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/

Websites

1. https://any.run/
2. https://www.broadcom.com/
3. https://www.cloudflare.com/
4. https://www.crowdstrike.com/en-us/
5. https://www.csoonline.com/
6. https://www.cisa.gov/
7. https://www.fortinet.com/
8. https://hacknjill.com/
9. https://www.ibm.com/us-en
10. https://ics-cert.kaspersky.com/
11. https://www.microsoft.com/en-us/
12. https://www.rapid7.com/
13. https://www.sentinelone.com/
14. https://www.techtarget.com/
15. https://www.nytimes.com/
16. https://totalmilitaryinsight.com/
17. https://www.trendmicro.com/en_us/business.html
18. https://www.weforum.org/

Mihai MELINTEI (1)
Lucian Blaga University of Sibiu, Romania
Mihaela COJOCARI (2)
Lucian Blaga University of Sibiu, Romania

ROMANIA'S LEGISLATIVE FRAMEWORK ON ENERGY SECURITY IN RELATION TO EU POLICIES

Abstract:	*European energy policy has transformed and evolved significantly over the last decades, responding to the global and regional challenges brought about by geopolitical, economic and geo-strategic changes. In terms of European legislation, the Union has developed a robust regulatory framework designed to respond to the challenges in the energy field, with a particular focus on the integration of the internal energy market and the promotion of renewable energy sources. For Romania, integration into the European Union has meant a series of adaptations of national legislation to European standards, with the aim of improving energy efficiency and increasing the security of energy supply. Measures include creating a diversified system of energy sources, interconnecting energy transmission networks with those of neighboring countries and developing energy storage capacity.* *In this paper, we aimed to identify the points of intersection between national and EU policies in the field of energy security. The identification of the rules that give this field a public character (in terms of overriding interest) and of the national legislative framework that would prioritize/not prioritize European policies, constitute two other points of interest for this paper.*
Keywords:	**Energy Security; legislative framework; energy policy; EU; geopolitics**
Contact details of the authors:	E-mail: mihai.melintei@ulbsibiu.ro (1) mihaela.cojocari@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Department of International Relations, Political Science and Security Studies** **Lucian Blaga University of Sibiu, Romania (1) (2)**
Institutions address:	Victoriei Boulevard Nr. 10, Sibiu, 550024, Romania (1) (2)

Introduction

Energy security is an important pillar not only in national security, but also at EU level and, like any other field, it based on a legislative framework[1]. Starting from this premise, we set out to analyze the legal norms that regulate the field of energy security and therefore, being topical for at least a decade, we have summarized important aspects of the situation in Romania, compared to the EU legislative structure at the European Union scale. It is essential to note from the outset that the subject itself is a challenge for us, since the field of energy security involves complex interdependencies between several national, regional and international regulatory levels, technological and geostrategic changes that have a direct impact on the stability and fluctuation of the energy system[2].

European energy policy has transformed and evolved significantly over the last decades, responding to the global and regional challenges brought about by geopolitical, economic and geo-strategic changes[3]. In

[1] Benjamin Sovacool, *Energy Security*, Vol. 4, SAGE Publications, London, 2013, p. 311
[2] Michèle Knodt, Jörg Kemmerzell, *Handbook of Energy Governance in Europe*, Springer International Publishing, Cham, 2022, p. 14
[3] Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New York, 2020, p. 25

terms of European legislation, the Union has developed a robust regulatory framework designed to respond to the challenges in the energy field, with a particular focus on the integration of the internal energy market and the promotion of renewable energy sources. For Romania, integration into the European Union has meant a series of adaptations of national legislation to European standards, with the aim of improving energy efficiency and increasing the security of energy supply. Measures include creating a diversified system of energy sources, interconnecting energy transmission networks with those of neighboring countries and developing energy storage capacity. A well-developed external energy policy also includes strategic partnerships with countries that have abundant energy resources and have also advantages from the stability and diversification of their markets, both European and international. A collaborative approach can therefore maximize economic and national security benefits. In this context, energy security becomes a multidimensional framework, including economic (referring to the impact on changes in the country's macroeconomic indicators), industrial and, finally, legislative aspects, or we cannot discuss an area without having some 'black and white' regulation to which we can refer. We appreciate that the legislative doctrine in the field of energy security is restricted, which makes us analyze the normative texts without starting from a pre-existing interpretation.

In this paper, we aimed to identify the points of intersection between national and EU policies in the field of energy security. The identification of the rules that give this field a public character (in terms of overriding interest) and of the national legislative framework that would prioritize/not prioritize European policies, constitute two other points of interest for this paper.

It is essential to find out whether, in terms of legislation on energy resources, the state has retained its authenticity, or whether we are talking about a transposition of legal norms from the regional to the restricted national card, where resources are elective in relation to other EU Member States. In other words, is it or is it not balanced to "transplant legal rules" regarding the constitution, development and exploitation of resources, as long as we cannot equalize their value at the level of EU Member States? Or, by transposing legal norms from other legal systems, we risk losing the essence of our own convictions in order to build a genuine legal foundation. The need for legal modernization, together with the lack of domestic legal resources, has also prompted legal importation. The urgency of building and consolidating the Romanian unitary national state and a pressing need for international legitimacy completed the panoply of causes of the Romanian "legal transplant"[1]. Starting from these challenges, we will try to see whether we can still speak of a national identity, corroborating the context of the state's energetic resources with the legal norms, to be able to state that identity is not just a set of colors of one's own being, reflected through the mirror in the hands of the other.

Certainly, this article has a subjective focus, and its own perspective found on the legal provisions in the field, as well as other bibliographical sources. Based on these, we intend to highlight important concepts of the developed theme.

Romania's legislative framework in the field of energy security

Like any other work involving a legislative interpretation, regardless of the field of regulation, the starting point will be the fundamental law of the State. In this respect, we have found that there are no express regulations on energy security in the constitutional text, but the content of some of the rules reveals the public nature of the resources that constitute the country's energy potential. This aspect is outlined by the provisions of Art. 136 of the Romanian Constitution on Property, especially (3) part: "The subsoil resources of public interest, the airspace, the waters of national interest with a appreciable energy potential, the beaches, the territorial sea, the natural resources of the economic zone and the continental shelf, as well as other assets established by organic law, are the exclusive object of public property"[2]. This is confirmed by paragraph (2) of the same article. In the same way, we note the duty of the State to guarantee and protect the resources that are subject to public ownership, as it is expressly stated: "Public property is guaranteed and protected by law and belongs to the State or to the administrative-territorial units"[3]. We mentioned in the introduction of the paper, the role of energy security for the country's economy, or in this case we find a regulation in the content of the fundamental law, as provided by art. 135, relevant being paragraph (2) letter d: "the exploitation of natural

[1] Manuel Guțan, *Rolul transplantului juridic în construcția dreptului public românesc modern și contemporan (teză de abilitare)*, Sibiu, 2017, p. 4

[2] CDEP, *Constituția României*, https://www.cdep.ro/pls/dic/site.page?id=339 (25.10.2024)

[3] *Idem*

resources, in accordance with the national interest"[1]. Attest to the two articles, we note that, on the one hand, the public nature of the rules governing the resources (including energy-generating resources) are of a public nature, and on the other hand, the state has the power to exploit the resources, *per a contrario*, the obligation to use them exclusively in the public interest. We appreciate that the area of public concern this case will be limited to the territory of Romania, or if we had a strict interpretation, we would ensure compliance with these rules, so that all the resources available to the country, not to satisfy any foreign interest, and in these cases we wonder, what does this foreign interest means and if we can actually discuss a common interest at the Union level, taking into account Community policies. With Romania's accession to the European Union, the state has undertaken to adapt the legislation and as much as possible to balance the legislative framework so that the concept becomes a whole. Title VI of Romania's Constitution begins with a complex article, which exemplifies with maximum clarity the aforementioned.

Consequently, Romania's entry into the foundational treaties of the European Union, aimed at delegating specific authorities to the Community institutions and jointly exercising the competencies outlined in these treaties with other Member States, will be achieved through a law passed in a joint meeting of the Chamber of Deputies and the Senate, requiring a two-thirds majority of the total Deputies and Senators. Due to accession, the rules of the Treaties that form the European Union and other obligatory Community regulations will override conflicting domestic law provisions, in accordance with the provisions of the Act of Accession. The regulations in paragraphs 1 and 2 shall equally apply, with necessary modifications, to the adoption of the acts amending the Treaties that establish the European Union. The Parliament, the President of Romania, the Government, and the judicial authority will ensure the implementation of the obligations arising from the Act of Accession and from the stipulations of paragraph 2.

The Government will send the draft binding acts to both Houses of Parliament prior to their submission for approval to the European Union institutions. We note that under this Article, once legal norms at the State level are found to be contrary to those at the Union level, we are talking about a priority of the Community ones. In other words, by referring to this provision, we understand to prioritize and apply EU policies also in the field of energy, which finds its place among the activities regulated by organic laws. The assumption of the State's obligation to respect in good faith the treaties to which it is a party is also reflected in the content of Article 11 of the Constitution, as these ratified conventions are recognized as part of domestic law[2].

Considering the above in relation to the constitutional provisions, in particular with regard to the treaties, and taking into account the status of a Member State of the European Union, we bring into the debate as sources of research for this paper the two fundamental treaties of the Community: TEU and TFEU. We therefore ask ourselves whether we can speak of a purely national or a common legal at the level of the Union in the field of energy. The essence of such an answer is also based on the legal rules, which expressly provide for competence for each area of activity, including energy[3].

The essence of such an answer is also based on the legal rules, which expressly provide for competence for each area of activity, including energy. Therefore, it is clearly stated in Article 194 of the Treaty on the Functioning of the European Union (TFEU)[4] that the European Union and its member states share responsibility for energy. Each Member State, however, is still free to set the terms under which its renewable energy resources can be used, as well as the overall composition of its energy supply.

Article 2 of the Treaty on the Functioning of the European Union defines three categories of competences[5]:

The Union and the Member States may enact laws and enact legally binding acts in a particular area when the Treaties grant the Union a joint competence with the Member States in that area. To the extent that the Union has not implemented its authority, the Member States will do so. To the extent that the Union has chosen to stop exercising its authority, the Member States will once more exercise their authority.

---

[1] *Ibidem*, Titlul IV, Art.135

[2] CDEP, *Constituția României*, https://www.cdep.ro/pls/dic/site.page?id=339 (25.10.2024)

[3] Anna Herranz-Surrallés, Israel Solorio, Jenny Fairbrass, *Renegotiating Authority in EU Energy and Climate Policy*, Routledge, New York, 2022, p. 51

[4] EUR-Lex, *Consolidated version of the Treaty on the Functioning of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT (27.10.2024)

[5] *Idem*

- Within the parameters established by this Treaty, which the Union can establish, the Member States will coordinate their employment and economic policies.
- According to the terms of the Treaty on European Union, the Union will have the authority to establish and carry out a common foreign and security policy, which will include the gradual development of a common defence strategy.
- Without displacing the Member States' authority in certain areas, the Union may take action to support, coordinate, or enhance their actions in specific areas and follow the guidelines outlined in the Treaties. Harmonizing the laws or regulations of Member States is not required by legally binding acts of the Union that are adopted based on the provisions of the Treaties pertaining to these areas.
- The scope of and arrangements for exercising the Union's competences shall be determined by the provisions of the Treaties relating to each area[1].

We note that although the Union can legislate in the energy field, the competence is limited, because the way of exploiting the resources remains within the discretion of the Romanian legislator. Recalling here the state's duty to use energy resources in the public interest, we conclude that if energy security declines, given that the country is in the category of states with potential, this will be due to a lack of responsibility on the part of the competent authorities.

We also mention here the legislative text on energy efficiency and specifically we refer to Law no.121/2014, which expressly provides for: energy efficiency policy (art.2)[2], procurement by public bodies (art.7)[3], energy efficiency measures (art.8)[4] and provisions on the information and awareness program for end customers (art.13)[5]. The content of art.2 exemplifies the aims pursued with a view to improving energy efficiency and we will mention a few of them listed by way of example in the second paragraph:[6] The national energy efficiency policy is an integral part of the State energy policy and aims to:

- removing barriers to the promotion of energy efficiency;
- promoting energy efficiency mechanisms and financial instruments for energy saving;
- educating and raising the awareness of final consumers on the importance and benefits of implementing energy efficiency improvement measures;
- cooperation between final consumers, producers, suppliers, energy distributors and public bodies in order to achieve the objectives set by the national energy efficiency policy;
- promoting fundamental and applied research in the field of energy efficiency"[7].

The five goals result, on the one hand, from the state's task to identify the obstacles to the implementation of new technologies in the field of energy security and, on the other hand, to create a favorable environment for private individuals to intervene with innovative proposals in the field. So, to support involvement through financial mechanisms (grants or subsidies). We consider that in this case we cannot see any violation of the public interest to the detriment of the private interest, *per a contrario*, such an incentive could result in ensuring efficiency focused on meeting national needs.

The solutions put forward by natural or legal persons with a view to ensuring energy efficiency should be assessed fairly and effectively. The legislator has mentioned in c let. another purpose which would be aimed at educating consumers, and we believe that one of the ways of implementation would be to organize training and information programs on the use of more efficient equipment. Also promoting policies in the industrial sector, which is one of the target consumers

[1] EUR-Lex, *Consolidated version of the Treaty on the Functioning of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT (27.10.2024)
[2] Portal Legislativ, *LEGE nr. 121 din 18 iulie 2014*, https://legislatie.just.ro/Public/DetaliiDocument/160331 (27.10.2024)
[3] CDEP, *Decret pentru promulgarea Legii privind eficiența energetică,* Monitorul Oficial No. 574/1 august 2014, https://www.cdep.ro/pls/legis/legis_pck.lista_mof?idp=23940 (27.10.2024)
[4] Portal Legislativ, *LEGE nr. 121 din 18 iulie 2014*, https://legislatie.just.ro/Public/DetaliiDocument/160331 (27.10.2024)
[5] *Ibidem*, Art.13
[6] *Ibidem*, Art. 2
[7] *Idem*

EU policies

The Treaty of Lisbon, which entered into force on December 1, 2009, makes substantive changes to the Treaty on European Union and the Treaty establishing the European Community, as well as to the Treaty establishing the European Atomic Energy Community, and provides the Union with the legal framework and legal instruments to meet future challenges and citizens' expectations[1]. Article 194 of the Treaty on the Functioning of the European Union stipulates that the Union's policy on energy, in a spirit of solidarity among Member States, shall aim to: ensure the functioning of the energy market; ensure security of energy supply in the Union; promote energy efficiency and energy saving, and the development of new and renewable energy sources; promote the interconnection of energy networks. The measures necessary to achieve these objectives to be decided by the EU Parliament and Council should be without prejudice to the right of a Member State to determine the conditions for exploiting its own energy resources.

The goals of the European Union's energy policy are outlined in Article 194 of the Treaty on the Functioning of the EU. These goals include ensuring the energy market operates as intended, ensuring the Union's energy supply is secure, encouraging energy conservation and efficiency, and fostering the development of new and renewable energy sources[2].

In December 2019, the European Commission unveiled the *European Green Deal* - its roadmap that aims to make Europe the first climate-neutral continent by 2050[3]. The roadmap seeks to guarantee a fair and inclusive transition while enhancing the EU's sustainability and competitiveness. Reducing greenhouse gas emissions is one of the EU's commitments, given the requirement that developed nations cut emissions collectively. The "Energy Roadmap 2050" of the Commission[4] explores the challenges of achieving the EU's decarburization goal while ensuring security of energy supply and competitiveness.

While aiming for a more effective and coordinated use of restrictive measures, the Union will use all available tools and options to protect its goals and objectives, which includes the territorial sovereignty and sovereign rights of Member States to exploit their natural assets in accordance with international law. It will also protect the EU's and its Member States' ability to make independent decisions on energy policy, rejecting economic restraint and interference from third parties[5].

The European Commission has conducted a thorough exercise to evaluate the durability of the EU's power supply framework to guarantee energy supply readiness for the winter of 2024–2025. It underwent extensive testing in exceptionally harsh conditions, accounting for the December 31, 2024, shutdown of gas transportation from Russia through Ukraine. The experiment demonstrated that the EU is equipped and ready to handle even the most extreme and improbable situations when it comes to gas supply security. Additionally, it offered data to strengthen the EU's energy assurance framework's resilience[6].

The exercise tested the measures adopted and reinforced over the last two years and looked at the interactions between the gas and electricity sectors. This 2024 exercise brought together around 70 participants representing most EU countries, as well as, for the first time, Ukraine, Moldova and the Energy Community Secretariat. Transmission system operators for gas and electricity, as well as ENTSOG and the European Network of Transmission System Operators for Electricity (ENTSOE), were also invited. The EU supports diverse and often cross-border energy infrastructure projects that produce, store and distribute energy efficiently. To accomplish our goals for energy and climate policy, this funding helps create an increasingly coordinated energy system. These initiatives help to lessen the EU's reliance on energy imports from foreign nations while also interconnecting energy systems and advancing the integration of clean technology and

[1] European Parliament, *Treaty of Lisbon*, https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-lisbon (04.11.2024)

[2] Ministerul Afacerilor Externe, *Politica energetică a Uniunii Europene*, https://www.mae.ro/node/1624 (04.11.2024)

[3] Helene Dyrhauge, Kristina Kurze, *Making the European Green Deal Work. EU Sustainability Policies at Home and Abroad*, Taylor & Francis, New York, 2024, p. 27

[4] Comisia Europeană, *Aplicarea în ţările UE*, https://commission.europa.eu/energy-climate-change-environment/-implementation-eu-countries_ro (02.11.2024)

[5] *Idem*

[6] European Commission, *The EU's energy security framework successfully tested to ensure winter preparedness*, 8.11.2024, https://energy.ec.europa.eu/news/eus-energy-security-framework-successfully-tested-ensure-winter-preparedness-2024-11-08_en (17.11.2024)

renewable energy sources into the EU energy system. The Energy Union responds to the main challenges facing the EU in the field of energy. These are:

- climate change: the EU has committed to climate neutrality by 2050, and reducing energy-related emissions is one of the key actions;
- energy dependence: as the world's largest energy importer, the EU needs to reduce its dependence on external markets;
- energy infrastructure: the EU needs to fully integrate its energy markets, modernize its energy infrastructure and ensure coordination of energy prices at national level[1].

In addition to providing EU customers and industry participants with more options and reduced costs, the establishment of a fully operational Energy Union helps strengthen the EU economy, energy security, and climate change commitment. The European Commission reports outline several aspects of Romania's energy security for the current period. It was assessed that the wholesale electricity and gas markets in Romania are strongly influenced by market interventions, which go beyond the expired framework established by the EU on emergency measures. In the identical vein, the Romanian government has put forth new energy security goals, which are incorporated into the Romania 2025–2035 Energy Strategy with an eye towards 2050. This paper lays out the basic goals and describes the vision for the growth of the country's energy industry. The report also lists the national, European, and international standards that impact and guide energy-related policies and choices. Global and regional economic, technological, and geopolitical changes are taken into consideration in the Energy Strategy, along with the main obstacles brought about by the need for a green transition, market volatility, and Romania's border position in the EU and NATO, along with the ongoing wars in the immediate area. Furthermore, the national energy sector must be able to meet all the Republic of Moldova's needs under any circumstances, as Romania's energy security is closely tied to that of the Republic of Moldova. Romania therefore hopes to strengthen its position as a regional energy security pillar[2]. Having a diversified energy mix, Romania has a considerable advantage, having sufficient natural, financial and human resources to modernize the energy sector, aligning it with the community objectives of achieving climate neutrality by 2050. This sector must be prepared to support economic growth and the transformation of the economy, thus contributing to improving the quality of life. All reform and modernization objectives consider accessibility, inclusiveness and economic competitiveness for citizens and industrial consumers that the energy sector serves. Romania benefits from a diversified energy mix, which provides a strong foundation for modernizing its energy sector. With abundant natural, financial, and human resources, the country is well-positioned to align its energy sector with the European Union’s goal of achieving climate neutrality by 2050.

The sector must be equipped to support both economic growth and the overall transformation of the economy, thereby improving the quality of life. All reform and modernization efforts are designed to ensure accessibility, inclusivity, and economic competitiveness for both citizens and industrial consumers served by the energy sector. Analyzing the content of the project, we note that there are several directions that focus on making an energy market more efficient, compared to Union standards, optimizing and sustaining heating systems. We exemplify here the third objective with reference to improving energy efficiency (EE) along the entire energy chain, including production, transportation, distribution and end-use of energy, which will generate environmental benefits, reduce greenhouse gas emissions, improve energy security, contribute to alleviating energy poverty and lead to an increase in the competitiveness of economic activity across all sectors of the economy.[3] Through the package of reforms recently adopted at European level, consumers throughout the EU and implicitly in Romania will be able to benefit from more stable energy prices, less dependence on the price of fossil fuels and better protection against future crises. As the energy sector undergoes this transformation, it is crucial to ensure a just transition for workers and communities’ dependent on traditional energy industries. Social inclusion and the creation of new employment opportunities in the green economy will be essential to achieving long-term success. Strengthening cooperation between the public and private

[1] European Commission, *European Sustainable Energy Week 2025: Commission opens applications to host a policy session,* https://energy.ec.europa.eu/news/european-sustainable-energy-week-2025-commission-opens-applications-host-policy-session-2024-11-05_en?prefLang=ro (28.10.2024)

[2] Mihai Melintei, *Energy security of the Republic of Moldova in the new international context. Risks and opportunities*, “Legea și Viața”, No. 4, Chișinău, 2023, pp. 61-69

[3] *Strategia energetică a României 2025-2035, cu perspectiva anului 2050*, p. 4, https://e-nergia.ro/wp-content/uploads/2024/06/Strategia_Energetica_vf_rev_1206-1.pdf (21.11.2024)

sectors, as well as fostering regional collaboration, will be key to addressing challenges and maximizing the potential benefits of this transition. Ultimately, Romania's energy strategy should focus on creating a sustainable, resilient, and competitive energy sector that not only meets the country's climate goals but also enhances the well-being of its citizens and contributes to the growth of a green economy

The key elements of this package, to be transposed or implemented at national level, will need to ensure:

- More stable and predictable energy prices, while ensuring the efficient functioning of the market and avoiding distortion of the Community market;
- Better preparedness for future crises;
- Protecting and strengthening the role of consumers;
- Ensuring security of supply.

In this context, the consumer will be empowered as a central actor in energy markets, able to manage their own consumption, produce their own energy or be part of an energy community. Romania's efforts to increase the share of renewable energy sources, increase energy efficiency, strengthen networks and adopt modern and digital technologies, with the goal of providing secure, affordable and clean energy for a competitive national economy, require a strong institutional environment and an appropriate corporate governance framework. This document proposes ways to strengthen institutions, improve corporate governance of state-owned energy companies, strengthen the regulatory framework, and align national policies and regulations with the EU framework[1].

Conclusions

Following the thread of my own work, I will exemplify some personal conclusions regarding the researched topic. Firstly, I found that the field of energy security is a point of interest both nationally and regionally, if we refer to the community framework of the European Union. The economic context of the country has as an influencing factor the development of the energy field. Energy security depends significantly on the interconnection of energy networks with other EU states, or the legislative framework constitutes the foundation of activities specific to the energy infrastructure. European energy policies, as promoted by the European Green Deal and various directives, have a significant impact on the member states, including Romania, in terms of the development and exploitation of energy resources[2].

These policies aim to reduce carbon emissions, promote renewable energy sources and guarantee security of supply. However, despite these common objectives, each member state retains the right to establish its own conditions for the exploitation of resources, which deepens the interdependence between European energy policy and national needs. Thus, Romania must balance the protection of its own resources with the objectives of the EU, to maximize economic and national security benefits. We state again the idea regarding the relationship between domestic and EU legislation on the energy sector and we consider that based on shared competence, the state will legislate on the mechanisms for exploiting its own resources, and as regards common policies for the creation of a single market, the margin of appreciation of the Member State is reduced to a minimum. Based on the legislative texts invoked, the state has the duty to act in the national interest, or in a contrary hypothesis, we will consider a violation of the constitutional provisions[3].

In the body of the paper, we have pleaded the European Union's policies in the energy area and, consequently, those of the Romanian state, as a fully-fledged member state. We are questioning whether there are intersections between the objectives of European energy policy, and in this regard, we mention the following goals applicable at the domestic level, which stem from the premises of the EU policy: the development of infrastructure in the field, the preparation of mechanisms for addressing crisis situations, and reducing dependence on external markets, referring here to third countries outside the European Union. The European Commission unveiled the "European Green Deal" in December 2019, which is a blueprint that aims to make Europe the first continent to achieve carbon neutrality by 2050. As a result, we see tangible progress in this area. According to the rules of the Constitution and the tenets set forth by the Treaty on European Union

[1] Ministerul Energiei, *Plan Strategic Instituțional*, https://energie.gov.ro/plan-strategic-institutional (04.11.2024)
[2] Neil Makaroff, *Turning the European Green Deal into Reality*, "Strategic Perspectives Brief", Brussels, 2022, p. 6
[3] Robert Rybski, *Energy in the European Green Deal: Impacts and Recommendations for MENA Countries*, "The Journal of World Energy Law & Business", Vol. 16, No. 2, Oxford, 2023, pp. 128-129

(TEU) and the Treaty on the Functioning of the European Union (TFEU), Romania has obliged to modify its national laws to conform to EU standards in energy security.

Romania has been forced to adhere to a common law that supersedes state provisions that deviate from EU standards because of its procedure of "transposing" European regulations. This highlights how interwoven the EU's energy system is. However, we believe that Romania still retains a margin of legislative freedom and preserves its autonomy over the management of its energy resources within its national heritage. While the European Union creates shared energy security policy, Member States are free to set their own terms for the extraction of renewable energies under Article 194 of the TFEU. Thus, Romania can shape its own national energy policy, but within a European legislative framework that promotes an interconnected internal energy market.

Bibliography

Books

1. Dyrhauge, Helene; Kurze, Kristina, *Making the European Green Deal Work. EU Sustainability Policies at Home and Abroad*, Taylor & Francis, New York, 2024
2. Herranz-Surrallés, Anna; Solorio, Israel; Fairbrass, Jenny, *Renegotiating Authority in EU Energy and Climate Policy*, Routledge, New York, 2022
3. Knodt, Michèle; Kemmerzell, Jörg, *Handbook of Energy Governance in Europe*, Springer International Publishing, Cham, 2022
4. Sovacool, Benjamin, *Energy Security*, Vol. 4, SAGE Publications, London, 2013
5. Yergin, Daniel, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New York, 2020

Articles

1. Makaroff, Neil, *Turning the European Green Deal into Reality*, "Strategic Perspectives Brief", Brussels, 2022
2. Melintei, Mihai, *Energy Security of the Republic of Moldova in the New International Context. Risks and Opportunities*, "Legea și Viața", No. 4, Chișinău, 2023
3. Rybski, Robert, *Energy in the European Green Deal: impacts and recommendations for MENA countries*, "The Journal of World Energy Law & Business", Vol. 16, No. 2, Oxford, 2023

Documents

1. *Constituția României*, https://www.cdep.ro/pls/dic/site.page?id=339
2. EUR-Lex, *Consolidated version of the Treaty on the Functioning of the European Union,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT
3. European Parliament, *Treaty of Lisbon,* https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/treaty-of-lisbon LEGE Nr. 121 din 18 iulie 2014, *privind eficiența energetică*, https://legislatie.just.ro/Public/DetaliiDocument/160331
4. *Strategia energetică a României 2025-2035, cu perspectiva anului 2050,* https://e-nergia.ro/wp-content/uploads/2024/06/Strategia_Energetica_vf_rev_1206-1.pdf

Web sources

1. http://www.commission.europa.eu/
2. http://www.energie.gov.ro/
3. http://www.energy.ec.europa.eu/
4. http://www.mae.ro/

Cristina ONEȚ
Lucian Blaga Univesity of Sibiu, Romania

ROMANIA`S ENERGY SECURITY IN THE CONTEXT OF COMBATING CLIMATE CHANGE

Abstract:	*Romania's energy security is an important and complex issue, as the paths to follow are sometimes winding, other times unclear, and always fluid, given that the core issues are constantly changing. This study aims to address as many aspects as possible that contribute to achieving this goal. Still, given the complexity of the subject, an exhaustive analysis cannot be carried out within a scientific approach of this nature. Therefore, the issue of Romania's energy security has been limited to the context created by European policies aimed at combating climate change.* *On the one hand, the study addresses the limitations imposed on member states by European regulations, which set out the milestones to achieve full neutrality regarding greenhouse gas emissions, a goal assumed by all member states by 2050.* *On the other hand, it analyzes the most important courses of action necessary to achieve and maintain energy independence, namely increasing and diversifying electricity production, identifying the optimal energy mix for Romania, improving the functioning of the electricity market, and, finally, the situation of the National Power Transmission System and its safety.* *Therefore, Romania must identify the appropriate measures that will allow it to achieve its fundamental strategic objective regarding energy security through means harmonized with the obligations it has undertaken as a member state of the European Union in combating climate change.*
Keywords:	**Energy security; electricity production; energy mix; liberalized energy market; combating climate change**
Contact details of the authors:	E-mail: cristina.onet@ulbsibiu.ro
Institutional affiliation of the authors:	**Law Faculty, Lucian Blaga Univesity of Sibiu, Romania**
Institutions address:	Calea Dumbrăvii 34, Sibiu, Romania 550324

Introduction

Energy security has been a matter of international concern for a long time. Once it became clear to modern society and the global economy that essential resources are limited and unevenly distributed, a continuous global struggle emerged to secure them. Over the past decades, we have witnessed a true clash between various state and non-state entities engaged in efforts to acquire such resources.

An exhaustive list of these resources is difficult to compile, so we will limit ourselves to mentioning only the most important categories:

a) Natural resources and raw materials;
b) Human resources;
c) Financial resources.

Efforts to attract or direct these resources also generate their circulation, meaning flows of raw materials, specialized human resources, and financial flows.

The methods and instruments through which the distribution of these resources at the international level can be influenced or controlled are extremely varied. Some of these instruments are general, such as strategic or programmatic documents or decisions established through international agreements, the legislative

framework of each state, public policies (national, regional, or international), financial instruments such as financial markets, financial flows and access to them, or financial mechanisms (such as carbon certificates or green certificates), and, last but not least, technical instruments like infrastructure networks and their accessibility, best available techniques, sustainable energy mixes, technical quality standards, and product labeling systems. In addition to these general instruments, other types of tools or spontaneous or induced circumstances can influence resource distribution and have a special character, such as political and armed conflicts resulting in wars, terrorist actions or even piracy, bankruptcies of key entities involved in resource distribution, and major natural or catastrophic events that can significantly impact resource distribution in specific regions and periods. Of course, this description of the current context is extremely brief, and how the global struggle for resources is waged is far more numerous and diverse. It is also evident to any observer (even a less experienced one) that some of the means used to direct resources are legal, while others are less so, with some being openly used, while others are carefully concealed.

This brief overview aims to establish the general context that manifests globally and affects Romania. Additionally, the current regional context compels Romania to identify short-, medium-, and long-term solutions. This includes European policies aimed at combating climate change and the war in Ukraine, both of which pose significant challenges to Romania's National Energy System. It is important to note that an energy system consists of the production, storage capacity, and transportation of electricity. It must be viewed as a whole, encompassing the production of raw materials such as coal, natural gas, and oil, as well as their transportation to support electricity generation. A state's energy security is ensured when it can fully guarantee and control the functionality of all these elements.

The European context regarding the energy and climate change mitigation

European policies aimed at combating climate change have significantly influenced Romania's energy situation. The continuous reduction, up to the complete cessation, of atmospheric pollution through greenhouse gas emissions by major European polluters has also forced Romania to adopt specific measures to reduce coal-based electricity production. As is well known, the European Green Deal[1] is both an action plan and a new growth strategy based on ambitious climate and environmental objectives. Europe aims to significantly reduce greenhouse gas emissions by 2030 and to become climate-neutral by 2050. Regulation (EU) 2018/1999 of 11 December 2018[2] on the governance of the energy union and climate action establishes that the energy union must focus on five dimensions:

a) energy security;
b) the internal energy market;
c) energy efficiency;
d) decarbonization;
e) research, innovation, and competitiveness.

Thus, the goal of a resilient energy union, centered on an ambitious climate policy, is to provide EU consumers, including households and businesses, with secure, sustainable, competitive, and affordable energy, as well as to encourage research and innovation by attracting investments, which implies a fundamental transformation of Europe's energy system. Such a transformation is closely linked to the necessity of maintaining, protecting, and improving environmental quality, as well as promoting the prudent and rational use of natural resources, especially by promoting energy efficiency, energy savings, and the production of energy from new renewable sources. This objective can only be achieved through coordinated action, combining both legislative and non-legislative acts at the EU, regional, national, and local levels.

According to European regulations, the energy governance mechanism must be based on long-term strategies and integrated national energy and climate plans. These must cover ten-year periods, and their development and implementation began in the decade 2021-2030 but must continue until the proposed goals are achieved. At the same time, action programs must be followed by intermediate national integrated reports on energy and climate to highlight the results obtained, identify appropriate corrections, and set future objectives. Therefore, the reports submitted by member states will be followed by the European Commission's

[1] European Commission, *The European Green Deal*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en (12.11.2024)
[2] EUR-Lex, *Regulation (EU) 2018/1999 of the European Parliament and Of the Council of 11 December 2018,* https://eur-lex.europa.eu/eli/reg/2018/1999/oj/eng (12.11.2024)

integrated monitoring measures so that all member states advance in the same direction and, as far as possible, at the same pace, ensuring that no one is left behind. As a result, according to Article 3 of Regulation (EU) 2018/1999[1], by 31 December 2019, then by 1 January 2029, and subsequently every ten years, each member state must notify the Commission of an integrated national energy and climate plan. Finally, it is useful for this analysis to highlight the provisions of Article 4, point (c) of Regulation (EU) No. 1999/2018, mentioned above, which states that the energy security dimension of member states must focus on the following priorities:

- Increasing the diversity of energy sources and energy supply from third countries, which could aim to reduce dependence on energy imports;
- Increasing the flexibility of the national energy system;
- Managing the reduction or interruption of the supply of an energy source to improve the resilience of regional and national energy systems, including setting deadlines for achieving objectives.

In addition to the provisions above, Regulation (EU) 2018/842 of the European Parliament and of the Council of 30 May 2018[2] on the reduction of annual greenhouse gas emissions by member states for the period 2021-2030 in order to contribute to climate actions in accordance with the commitments made under the Paris Agreement mentions in its recitals that the transition to clean energy requires changes in investment behavior and the provision of incentives across the entire spectrum of policies. Thus, a key priority for the Union is the creation of a resilient energy union that provides its citizens with secure, sustainable, competitive, and affordable energy. To achieve these objectives, the Just Transition Mechanism was created at the European level, mobilizing over 100 billion euros for the 2021-2027 period to be directed toward the most affected regions or economic activities whose resilience is considered imperative, as is the case in the energy sector.

Romania's perspective of energy security

As a member state of the European Union, Romania has undertaken the task of complying with European legislation on combating climate change. This commitment has been translated into legislative, administrative, economic-financial, and technical measures aimed at enabling the government and other competent authorities to strike the right balance between the obligations assumed at the European level and Romania's need for energy security and stability.According to Law No. 123/2012 on Electricity and Natural Gas[3] the national energy strategy defines the objectives of the electricity sector in the medium and long term and the most efficient ways to achieve them, ensuring the sustainable development of the national economy and meeting energy needs, as well as providing a decent standard of living in terms of quality, both in the present and in the medium and long term, at an affordable price.

The energy strategy is developed by the relevant ministry in consultation with representatives of the energy industry, non-governmental organizations, social partners, and business representatives and is approved by the government. The energy strategy is periodically revised at the initiative of the relevant ministry, without compromising the stability and predictability essential to such a document, with the revised version being approved by the law[4]. At the same time, Law No. 123/2012 establishes that energy policy follows the directions set by the energy strategy and is implemented by the relevant ministry based on the government program, for a medium-term period, considering likely long-term developments, in consultation with economic operators in the electricity sector, non-governmental organizations, social partners, and business representatives[5]. Thus, according to the law, Romania's energy policy primarily focuses on the following directions of action:

---

[1] *Idem*

[2] Council of the European Union, European Parliament, *Regulation (EU) 2018/842 on binding annual greenhouse gas emission reductions by Member States from 2021 to 2030*, https://leap.unep.org/en/countries/eu/national-legislation/regulation-eu-2018842-european-parliament-and-council-binding#:~:text=This%20Regulation%20lays%20down%20obligations%20on%20Member%20States,sectors%20covered%20by%20article%202%20of%20this%20R (12.12.2009)

[3] *Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale*, Article 4, Paragraph 1, "Monitorul Oficial al României", No. 485, 16 Iulie 2012

[4] *Idem*

[5] *Idem*

a) establishing an appropriate institutional framework by defining the bodies and authorities responsible for implementing this policy;

b) ensuring the legal framework necessary for the safe and stable operation of the National Energy System (SEN);

c) ensuring the security of supply with fuel and electricity and the operational safety of the SEN;

d) ensuring environmental protection and ecological reconstruction of sites affected by energy activities;

e) ensuring transparency in fuel and energy prices and tariffs;

f) increasing energy efficiency;

g) promoting energy from renewable sources, unconventional sources, high-efficiency cogeneration, and energy storage, with priority given to supplying electricity to isolated settlements;

h) developing international energy cooperation, participating in regional and European energy markets to achieve a single energy market at the EU level, and ensuring the secure and safe operation of the SEN.[1]

Furthermore, the same legal framework, referring to Romania's energy security, stipulates in Article 5 that the government is responsible for determining, in collaboration with other state institutions and authorities, mandatory measures for all economic operators in the electricity sector, regardless of ownership, to maintain continuous energy production and supply, as well as any other measures concerning the safety and security of the SEN's operation[2]. To ensure the safe operation of the SEN, based on adequacy assessments conducted by the transmission and system operator, the competent authorities may take necessary measures to develop and implement mechanisms to secure energy capacities, aiming to achieve the desired level of adequacy in compliance with and aligned with the specific provisions of current European and national regulations[3]. In practical terms, Romania's energy security is considered a critical component of the country's national security. However, an analysis of this aspect should focus on several key factors, such as:

a) ensuring a large enough/sufficient quantity of energy from domestic production to meet the needs of the economy and the population;

b) maintaining a balanced and diverse internal energy production mix that guarantees a secure energy supply under any circumstances;

c) having rapid, easy, and affordable access to electricity from external markets;

d) fostering a domestic electricity market that is free, fair, stable, and functional;

e) developing complete, secure, and operational energy infrastructure networks of all types.

Romania's energy independence

The first element to consider when analyzing Romania's energy security is the degree of energy independence. It must be noted that Romania has not yet achieved this objective, as it has not been able to meet the energy needs of its economy and population solely from domestic production. However, the share of electricity imports is not very high. This share is continuously correlated with both the level of domestic production and consumption. Of course, the level of consumption also fluctuates depending on various circumstances, such as climatic factors, as well as economic, social, political, or even technical aspects. It is well known that climatic, meteorological, or natural events can cause significant fluctuations in both energy production and electricity consumption.

At the same time, Romania has set a strategic objective to achieve full energy independence by 2035. This would require that energy production significantly exceeds consumption so that, regardless of external factors, Romania can independently produce the necessary electricity, as a part of the Romania`s energy independence. It is well known that green energy sources are directly dependent on various external factors such as light intensity, wind strength, tides, or precipitation, making them unstable, and a high share of these sources could compromise domestic electricity production. For this reason, the National Energy System (SEN) must maintain a high proportion of stable electricity sources to ensure the security and stability of the entire system. In Romania, this refers to thermal electricity production.

Greenhouse gas emission measurements from coal-fired power plants have shown high levels of emissions, which create unhealthy living conditions in these regions. At the same time, the pollution levels

[1] *Ibidem,* Article 4, Paragraph 2, published in Monitorul Oficial al României, No. 485/16 of July 2012

[2] *Ibidem,* Article 5, Paragraph *2*, published in Monitorul Oficial al României, No. 485/16 of July 2012

[3] [3] *Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale*, Article 4, Paragraph 1, "Monitorul Oficial al României", No. 485, 16 Iulie 2012

generated by coal-fired power plants in Romania are in total contradiction with European policies to combat climate change. Given this reality and to maintain the stability of SEN and Romania's energy security, it has been decided through the strategic documents mentioned earlier that the capacities for electricity and heat production in coal-fired power plants will gradually be modernized and replaced with natural gas-based power plants. This transition is even more feasible as new natural gas explorations in the Black Sea Continental Shelf are expected to begin by the end of 2025. This refers to the Neptun Deep perimeter[1], whose first natural gas production is estimated for 2027.

Neptun Deep is Romania's first and largest offshore deepwater exploration project, with a surface area of 7,500 square kilometers, located about 160 km from the shore, in waters with depths ranging from 100 to 1,000 meters. According to information provided by OMV Petrom[2] the investment volume required for the project's development is estimated at 4 billion euros, and the natural gas deposit in this perimeter is estimated at approximately 100 billion cubic meters, making Romania the largest natural gas producer in the European Union.

This natural gas exploration project involves two major companies, namely Romgaz and OMV Petrom, with OMV Petrom being the operator of the Neptun Deep perimeter. Both companies have equal participation, each holding a 50% stake[3]. OMV Petrom is a company in which OMV Aktiengesellschaft (one of the largest publicly listed industrial companies in Austria) holds 51.2% of the shares, while the remaining 6.4% are owned by other foreign investors. Alongside foreign shareholders, OMV Petrom also has Romanian shareholders, who own over 42% of the shares. Of these, the Romanian state, through the Ministry of Energy, holds 20.7%, and 21.7% are owned by Romanian pension funds, in addition to nearly 500,000 individual investors and other Romanian entities.

The second partner in the Neptun Deep Project is the National Natural Gas Company "Romgaz" S.A. (S.N.G.N. ROMGAZ S.A.), a public enterprise and Romania's largest producer and main supplier of natural gas. The company is listed on the Bucharest Stock Exchange (BVB) and the London Stock Exchange (LSE). The main shareholder is the Romanian state, with a 70% stake. The company has extensive experience in the exploration and production of natural gas, with a history dating back over 100 years to 1909. Romgaz conducts geological exploration to discover new gas deposits, produces methane gas by exploiting the deposits in its portfolio, stores natural gas underground, performs interventions, major repairs, and special operations on wells, and provides professional technological transport services. In 2013, Romgaz expanded its field of activity by acquiring the Iernut thermal power plant and becoming a producer and supplier of electricity. On August 1, 2022, Romgaz became the sole shareholder of Romgaz Black Sea Limited, initially established by ExxonMobil Exploration and Production Romania Limited, following the completion of the acquisition and transfer of all shares representing 100% of this company's capital. Consequently, Romgaz Black Sea Limited is a subsidiary of Romgaz and holds 50% of the rights acquired and obligations assumed under the concession agreement for petroleum exploration, development, and exploitation in the Neptun Block XIX, Deepwater Zone of the Black Sea[4].

Given the ownership structure of the two companies involved in the Neptun Deep Project, it can be observed that the Romanian state holds a dominant corporate position, which can generate stability and security both for the conduct of extraction operations and for Romania's overall energy security. It should also be noted that oil and gas exploitation in the Black Sea Continental Shelf is not a new activity, as it began in the 1980s. Several companies hold petroleum agreements for the exploration and exploitation of hydrocarbons in the Black Sea, specifically in Romania's territorial waters.

Since the Neptun Deep deposit alone offers stability and energy independence for the next 20–30 years, without considering other exploitations, Romania's energy independence is achievable in a relatively short time frame. It should be mentioned that there are currently nine perimeters in the Romanian sector of the Black

[1] Offshore Technology, *Neptun Deep Gas Fielad Project, Black See*, https://www.offshore-technology.com/projects/neptun-deep-gas-field-project-black-sea/ (12.12.2024)

[2]OMV Petrom, Neptun Deep, https://www.omvpetrom.com/ro/activitatile-noastre/explorare-si-productie/neptun-deep (28.10.2024)

[3]Consilium Policy Advisors Group, *Neptun Deep: A 4-billion-euro investment*, https://www.omvpetrom.com/services/downloads/00/omvpetrom.com/1522243280403/sinteza-studiu-de-impact-cpag.pdf (28.10.2024)

[4] Romgaz, *Romgaz Black Sea Limited*, https://www.romgaz.ro/romgaz-black-sea-limited (12.11.2024)

Sea Continental Shelf that have been concessioned to companies exploring new natural gas and oil deposits. These include eight companies that hold various shares in concession agreements for Black Sea perimeters, according to information provided by the National Authority for Regulation in Mining, Petroleum, and Geological Storage of Carbon Dioxide (ANRMPSG)[1].

Romania's energy mix

Romania's energy mix represents the structure of its domestic electricity production. This mix is monitored and publicly reported in real-time by Transelectrica[2] making it impossible to provide an exact snapshot, as it undergoes constant fluctuations over short intervals (within minutes). Although this information is highly fluid, to assess whether Romania has a balanced energy mix, we present a sample from November 2024, based on official data:

- Hydrocarbon-based energy (natural gas): approximately 25%;
- Coal-based energy: approximately 17%;
- Nuclear energy: approximately 23%;
- Hydropower: approximately 23%;
- Wind energy: approximately 10%;
- Photovoltaic (solar) energy: approximately 2%.

Even though this presentation is approximate, we can make several observations regarding Romania's energy mix:[3]

- The energy mix is diversified, which provides flexibility and stability, even in circumstances where one or more green energy sources are affected.
- The share of various energy sources is relatively balanced, contributing to the stability of the energy system.
- There is significant potential for the development of renewable energy sources**.**
- Stable energy sources hold a substantial share (such as hydrocarbons and nuclear energy), which, although not renewable, are less polluting than coal-based energy and provide stability in electricity production.

National energy infrastructure networks

Energy infrastructure networks primarily consist of electricity transmission networks and oil and natural gas transport networks. Given the scope of this scientific endeavor, an exhaustive analysis of all categories of critical and non-critical infrastructure is not possible. Therefore, we will focus on the electricity transmission network, as it is a vital component of Romania's energy security and the broader energy union being developed at the European level[4].

An important point to highlight is that in Romania's National Energy System (SEN), the electricity generation, transmission, and distribution activities are completely separated. This separation was formalized by Government Decision No. 627/2000[5], which established the National Electricity Transmission Company "Transelectrica" S.A. as a distinct entity from other state companies responsible for electricity generation and distribution. Transelectrica is a state-owned joint-stock company considered of strategic national interest. Transelectrica manages the transmission of electricity through the Electricity Transmission Network (ETN)**,**

[1] The National Authority for Regulation in the Field of Mining, Petroleum, and Geological Storage of Carbon Dioxide (ANRMPSG), *Petroleum Agreements*, https://www.namr.ro/resurse-de-petrol/acorduri-petroliere/ (12.11.2024)

[2] Transelectrica, *The National Energy System*, https://www.transelectrica.ro/web/tel/sistemul-energetic-national, (14.11.2024)

[3] Cristina Oneț, *Greenhouse gas emission certificates-financial instruments for implementing environmental policies in Romania, "Pandemic Challenges for European Finance. Business and Regulation"*, Editirta Universității "Alexandru Ioan Cuza" din Iași, 2021, pp. 330-348

[4] European Commission, *A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy*, 2015, https://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0012.03/DOC_1&format=PDF (14.11.2024)

[5] Legislație.just, *HOTĂRÂRE nr. 627 din 13 iulie 2000 (*actualizată*) privind reorganizarea Companiei Naţionale de Electricitate - S.A. (actualizată până la data de 9 august 2010*),* HG 627 13/07/2000 - Portal Legislativ (12.12.2024)

which consists of 81 substations and 8,834 km of transmission lines**.** The ETN is classified as a national and strategic network, with a nominal line voltage of over 110 kV[1].

Since Transelectrica is responsible for managing the ETN, the company has also developed a 10-year ETN development plan, approved in 2022 and set to be completed by 2031. This plan is based on Romania's government strategies and public policies, future scenarios for the evolution of the National Energy System, and the objectives of the European Union's new policy for competitive, secure, and sustainable energy[2]. At the European level, consolidated legislation has been adopted to facilitate the development of an integrated European electricity market. To ensure its full functionality, Regulation 2019/941 on risk preparedness was adopted to enhance preparedness for risks by encouraging cooperation between transmission system operators (TSOs) within the EU, neighboring countries[3], and the Agency for the Cooperation of Energy Regulators (ACER)[4]. This regulation facilitates cross-border management of electricity networks during an energy crisis through newly created regional operational centers under Regulation (EU) 2019/943 on the internal electricity market.

The European Network of Transmission System Operators for Electricity (ENTSO-E) develops and proposes a common methodology for identifying risks, in collaboration with ACER and the Electricity Coordination Group, which is later approved by ACER[5]. Four sets of measures have been proposed:

- Common rules for preventing and preparing for electricity crises to ensure cross-border cooperation;
- Common rules for crisis management;
- Common methods for assessing supply security risks;
- A common framework for better evaluating and monitoring electricity supply security**.**

The electricity market in Romania

In June 2019, the European Union adopted the fourth energy package, which includes Directive 2019/944 on electricity and three regulations: EU Regulation 943/2019 on electricity[6] EU Regulation 941/2019 on risk preparedness[7] and EU Regulation 942/2019 on the Agency for the Cooperation of Energy Regulators (ACER)[8]. This was followed by the fifth energy package, titled "Implementing the European Green Deal," which was published on July 14, 2021, to align EU energy sector objectives with new EU climate goals for 2030 and 2050[9]. As a result, national legislation was modified accordingly, and the new provisions were subsequently implemented.

In accordance with European regulations, the National Energy Regulatory Authority (ANRE) was established at the national level. ANRE is an autonomous administrative authority, with legal personality, under parliamentary control, fully funded from its revenue, and independent in decision-making, organization, and function. Its responsibilities include the development, approval, and monitoring of the application of

---

[1] Transelectrica, *Management RET*, https://www.transelectrica.ro/ro/web/tel/date-generale-management (14.11.2024)

[2] Transelectrica, *The European Ten-Year Network Development Plan (TYNDP)*, https://web.transelectrica.ro/noutati/noutati/word/PPDRET%202024-2028-2033.pdf (15.11.2024)

[3] *Regulation 2019/941 on risk preparedness*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0001.01.ENG#:~:text=This%20Regulation%20sets%20out%20a%20common%20framework%20of,are%20taken%20in%20a%20coordinated%20and%20effective%20manner (15.11.2024)

[4] Agency for the Cooperation of Energy Regulators (ACER), *EU Regulation No. 942/2019*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R0942 (15.11.2024)

[5] https://www.entsoe.eu/ (15.11.2024)

[6] European Parliament and of the Council, *Regulation (EU) 2019/943 on electricity*, 2019, https://www.europex.org/eulegislation/electricity-regulation/#:~:text=Regulation%20%28EU%29%202019%2F943%20on%20the%20internal%20market%20for,role%20of%20the%20market%20in%20providing%20price%20signal 3A32019R0942 (15.11.2024)

[7] European Parliament and of the Council, *Regulation (EU) 2019/941 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC*, 2019, https://eur-lex.europa.eu/eli/reg/2019/941/oj/eng (15.11.2024)

[8] European Parliament and of the Council, *Regulation (EU) 2019/942 establishing a European Union Agency for the Cooperation of Energy Regulators*, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A158%3ATOC&uri=uriserv%3AOJ.L_.2019.158.01.0022.01.ENG (15.11.2024)

[9] *The European Green Deal*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/delivering-european-green-deal_en (15.11.2024)

mandatory regulations at the national level necessary for the functioning of the electricity, thermal energy, and natural gas sectors and markets, ensuring efficiency, competition, transparency, and consumer protection[1].

According to the Law No. 123/2012 on Electricity and Natural Gas[2], ANRE monitors the implementation of rules related to the roles and responsibilities of transport and system operators, distribution operators, suppliers, consumers, and other market participants. ANRE also monitors the management of congestion within the national electricity systems and the implementation of congestion management rules. In this regard, transport and system operators or market operators present ANRE with their congestion management rules, including capacity allocation rules, and ANRE has the right to review and request modifications to these rules. The rules for congestion management within interconnection capacities are established by all regulatory authorities or by the Agency for the Cooperation of Energy Regulators (ACER)[3].

At the same time, Article 20 of Law No. 123/2012 on Electricity and Natural Gas firmly establishes that the electricity market is competitive, and transactions in electricity are conducted on a wholesale or retail basis[4]. According to Article 21 of Law No. 123/2012 on Electricity and Natural Gas**,** participants in the electricity market must comply with the operating rules issued by ANRE, being required to assume financial responsibility for imbalances they generate on the electricity market. Additionally, market participants must notify the transport and system operator of imports, exports, and transit activities during trading periods, with external partners, for each border[5].

Market participants have the right to trade electricity as close as possible to real-time, and at least until the closing time of the intraday market, with the possibility to trade electricity in time intervals at least as short as the imbalance settlement period, both on the day-ahead markets and intraday markets[6].

To provide protection to market participants against price volatility risks based on the market and reduce uncertainty regarding future investment returns, long-term risk-hedging products are traded on the exchange transparently, and long-term supply contracts can be negotiated in over the counter (OTC) markets, subject to compliance with EU competition law. The designated electricity market operator offers products for trading on the day-ahead and intraday markets that are of sufficiently small size, with the minimum offer size being 500 kW or less, to allow the effective participation of dispatchable consumption, energy storage, and small-scale renewable energy sources, including direct participation by consumers.

Participation in any electricity market is voluntary. On the electricity market, the transmission and system operator purchase system services, including capacity and energy services.[7] On the retail market, suppliers sell electricity to final customers through bilateral contracts, at negotiated prices or prices set by standard offers[8]. Romanian authorities, together with participants in the domestic energy market (e.g., OPCOM**,** Transelectrica, etc.), are involved in initiatives aimed at facilitating the integration of the electricity market at the regional level, particularly in the process of implementing Regulation (EU) No. 1222/2015 establishing guidelines for capacity allocation and congestion management[9] in the context of creating and operating the Single Day-Ahead Coupling (SDAC) and Single Intra-Day Coupling (SIDC)**,** including the relevant contractual framework.

In Romania, the Electricity Market Operator (OPCOM) is a joint-stock company with 100% state-owned capital, established by Government Decision No. 627/2000.[10] The shareholding structure is as follows: 97.84%

---

[1] *Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale*, Article 7, "Monitorul Oficial al României", No. 485, 16 Iulie 2012

[2] *Idem*

[3] *Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale*, Article 7, Paragraph 1, "Monitorul Oficial al României", No. 485, 16 Iulie 2012

[4] *Ibidem*, Article 20

[5] *Ibidem*, Article 21

[6] *Ibidem*, Article 23, Paragraph 3

Ibidem, Article 23, Paragraph 7

[8] *Ibidem*, Article 23, Paragraph 8

[9] European Parliament and The Council, *Regulation (EU) 2015/1222 establishing guidelines for capacity allocation and congestion management*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R1222 (15.11.2024)

[10] Romanian Government, *Decision No. 627 of July 13, regarding the reorganization of the National Electricity Company - S.A.*, https://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=25333 (11.11.2024)

of the capital belongs to the National Electric Power Transmission Company - Transelectrica S.A., and 2.16% belongs to the Romanian State, represented by the General Secretariat of the Government[1]. Since September 2000, the wholesale electricity market and system services in Romania have been managed by S.C. OPCOM S.A. under the primary and secondary legislation in force. According to this, the Electricity and Natural Gas Market Operator "OPCOM" S.A. fulfills the role of administrator of the electricity market, providing an organized, viable, and efficient framework for conducting commercial transactions on the wholesale electricity market. It also manages centralized markets in the natural gas sector, ensuring consistency, fairness, objectivity, independence, impartiality, transparency, and non-discrimination[2]. The main activities conducted by OPCOM in the electricity sector, by the provisions of the primary legislation (Law No. 123/2012 on Electricity and Natural Gas) and secondary legislation (Government Decision No. 627/2000 on the reorganization of the National Electricity Company S.A.), are as follows:

- Organizing and managing centralized electricity markets;
- Acting as a clearing operator, carrying out clearing operations for the Day-Ahead Market (PZU) and Intraday Market (PI), determining payment obligations and/or collection rights for the Balancing Market and managing quantitative and financial imbalances for the responsible balancing parties;
- Organizing and administering the Green Certificate Market;
- Administering the platform for trading greenhouse gas emission certificates;
- Managing centralized markets in the natural gas sector;
- Monitoring the functioning of the markets managed;
- Collecting and publishing statistical market data, by the provisions of the Energy Law.

From the perspective of its area of activity and the responsibilities assigned to it, OPCOM is a member of the International Association of Power Exchanges (APEx), the Association of European Energy Exchanges (EUROPEX), and other national committees and associations. To ensure the quality of services provided under its licenses to third parties and involved authorities, OPCOM implements a Quality Management System certified by Lloyd's Register Quality Assurance. Additionally, to ensure the security, confidentiality, and availability of information to interested parties, OPCOM applies an Information Security Management System certified by Lloyd's Register LRQA[3].

Moreover, OPCOM undertakes necessary actions to fulfill its mission of providing reference prices for electricity and natural gas and forward price signals for electricity and natural gas, while ensuring the market conditions necessary for achieving the objectives of the National Energy Strategy. These actions aim to increase transparency and the overall integrity of the Romanian wholesale energy market, supporting the process of completing market liberalization and its integration into the European Single Market. Thus, OPCOM organizes and supervises the following specialized electricity markets:

a) Day-Ahead Market (PZU);
b) Intraday Market (PI);
c) Centralized Bilateral Contract Market - PCCB-NC trading method;
d) Centralized Double Continuous Bilateral Contract Market for Electricity (PC-OTC);
e) Centralized Universal Service Market (PCSU);
f) Centralized Renewable Energy Electricity Market Supported by Green Certificates (PC-ESRE-CV);
g) Centralized Anonymous Spot Market for Green Certificates (PCSCV).[4]

Conclusions

This study does not aim to provide a comprehensive analysis of Romania's National Energy System, as the topic would be too complex to cover in such a context. However, it offers an objective and well-argued overview of this system to assess whether Romania will be able to benefit from stable and real energy security within a short time frame.

Based on all the arguments presented throughout this work regarding each of the elements that determine the energy security of a country, we believe that Romania has set a realistic goal, with a high

[1] *Idem*
[2] *Idem*
[3] *Idem*
[4] *Idem*

potential for achievement. Although there are still actions to be taken, such as expanding and strengthening energy sources and transmission networks, improving the energy mix, and, finally, deeply and fully liberalizing the domestic market, as well as accessing other energy markets, the country is on the right path to achieving its energy security objectives.

Bibliography

Chapter Volume

1. Oneț, Cristina, *Greenhouse gas emission certificates-financial instruments for implementing environmental policies in Romania*, in Tofan, Mihaela; Bilan, Irina; Cigu, Elena, *Pandemic Challenges for European Finance. Business and Regulation*, Editura Universității ”Alexandru Ioan Cuza” din Iași

Documents and Legislation

2. European Parliament and of the Council, *Regulation (EU) 2019/941 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC*, 2019
3. European Parliament and of the Council, *Regulation (EU) 2019/942 establishing a European Union Agency for the Cooperation of Energy Regulators*, 2019
4. European Parliament and of the Council, *Regulation (EU) 2019/943 on electricity*, 2019
5. European Parliament and The Council, *Regulation (EU) 2018/1999, regarding the governance of the Energy Union and climate actions*, 2018
6. European Parliament and The Council, *Regulation (EU) 2018/842 on the mandatory annual reduction of greenhouse gas emissions by Member States in the period 2021-2030, in contribution to climate actions for meeting the commitments under the Paris Agreement*, 2018.
7. European Parliament and The Council, *Regulation (EU) 2015/1222 establishing guidelines for capacity allocation and congestion management*, 2015
8. European Commission, *Energy Union Strategy, published by the in 2015*, Brussels, 2015
9. Romania Legislative, *Law no. 123/2012 on electricity and natural gas, 2012*
10. Romania Government, *Decision No. 627 of July 13, regarding the reorganization of the National Electricity Company - S.A.*, 2000
11. European Commission, *A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, 2015*
12. European Network of Transmission System Operators for ElectricityEuropean, *Ten-Year Network Development Plan 2010-2020*

Websites

1. https://commission.europa.eu/
2. https://www.entsoe.eu/
3. https://www.namr.ro/
4. https://www.omvpetrom.com/
5. https://www.opcom.ro/compania/ro
6. https://www.romgaz.ro/
7. https://www.transelectrica.ro/

Mihai MELINTEI (1)
Lucian Blaga University of Sibiu, Romania
Iuliana NEAGOȘ (2)
Lucian Blaga University of Sibiu, Romania

THE EVOLUTION AND THE PERSPECTIVES OF THE OFFSHORE PROJECT "EX-30 TRIDENT" IN THE BLACK SEA

Abstract:	*Considering the significant potential of offshore natural gas reserves in the Black Sea, which could become commercial exploitations in the coming years, the discussion on the growing development of offshore activities has turned into a key regional strategic issue. This factor is mostly motivated by its indisputable impact on Southeast Europe's economy and energy security, but it is also influenced by the complexity of developments within the European energy market.* *In this regard, the Lukoil company, the concessionaire of the Trident offshore perimeter in the Black Sea, with estimated reserves of 30 billion m^3, in 2023 received approval from the Romanian National Agency for Mineral Resources, regarding the continuation of the deposit exploration program until 2026. However, Lukoil has not commercially validated its natural gas reserves of the Trident perimeter in the Black Sea, and against the background of military developments in Ukraine and sanctions against Russia, which have directly affected Lukoil's activity in EU member countries, the state of affairs remains uncertain.* *Moreover, in 2020, Lukoil put up its 87.8% stake in the Trident offshore project for sale. Based on these developments, the need to understand and research the perspectives of the Trident offshore project in the Black Sea is emerging. In addition, understanding and designing strategies for well-defined energy projects contributes to resilience in the face of crises, ensuring a balanced transition to sustainable and secure energy security.*
Keywords:	**Energy Security; Trident; offshore; natural gas; Black Sea**
Contact details of the authors:	E-mail: mihai.melintei@ulbsibiu.ro (1) iuliana.neagos@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Department of International Relations, Political Science and Security Studies** **Lucian Blaga University of Sibiu, Romania (1) (2)**
Institutions address:	Victoriei Boulevard Nr. 10, Sibiu, 550024, Romania (1) (2)

Introduction

Energy security has become a central topic in international debates, having a direct impact on the economic, political and social stability of states around the world. In the current global context, characterized by increasing geopolitical tensions, climate change and an accelerated transition to renewable energy sources, the challenges in the field of energy security are more obvious than ever. One of the most significant aspects of energy security is the dependence of countries on fossil resources, especially oil and natural gas[1]. Recent crises, such as the conflict in Ukraine, have revealed the vulnerabilities of European countries that rely on energy imports from Russia. This has led many states to reconsider strategies to diversify energy sources and look for alternatives to reduce dependence on traditional suppliers. At the same time, rising energy prices have put pressure on national economies, affecting both consumers and industries, which has raised concern for energy stability[2].

[1] Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New York, 2020, p. 20
[2] *Ibidem*, p. 21

On the other hand, in the context of the energy transition, many states aim to reduce greenhouse gas emissions and implement transition policies towards green energy sources. This transition, while environmentally necessary, brings with it challenges related to infrastructure, technology and investment. Such rapid change can generate instability in energy markets, especially in regions that still depend on fossil fuels. Thus, energy security in the current international context proves to be a complex issue, influenced by geopolitical, economic, and ecological factors. The challenges are significant, but the opportunities for innovation and international cooperation are equally great. Strategic approaches aimed at diversifying energy sources, promoting energy efficiency, and investing in energy projects and renewable technologies are essential to ensure a stable and sustainable energy future[1].

Considering the significant potential of offshore gas reserves in the Black Sea, which could become commercial exploitations in the coming years, the discussion on the evolution of offshore activities has become a matter of regional strategic significance. This aspect is primarily driven by its undeniable effect on the economy and energy security of the Southeast Europe region, but also in the context of the complexity of changes within the European energy market. In the past decade, the consumption of natural gas has risen significantly, according to IEA data, which has led to the redevelopment of energy projects in the offshore sector of the Black Sea. In this context, Lukoil, the concessionaire of the Trident offshore perimeter in the Black Sea, with estimated reserves of 30 billion m^3 of gas, in 2023 received approval from the National Agency for Mineral Resources of Romania, regarding the continuation of the exploration program for the deposits until 2026[2].

However, Lukoil hasn't commercially verified the natural gas reserves within the Black Sea's Trident perimeter. Given the backdrop of military actions in Ukraine and sanctions imposed on Russia, which had a direct impact on Lukoil's operations in EU member states, the situation is still unclear. Furthermore, Lukoil offered an 87.8% share in the Trident offshore project for sale in 2020. Therefore, it is necessary to examine the project's development and prospects.

Evolution of the Trident offshore project

Offshore natural gas energy projects have become increasingly important in the global energy landscape, contributing significantly to the energy security of countries and regions[3].

In July 2010, Lukoil Overseas Atash B.V., together with the company Vanco International Ltd., were declared the winners of the exploration-development license for hydrocarbon deposits in the perimeters EX-29 Rapsodia and EX-30 Trident, located in the territorial waters of Romania in the Black Sea, following the X round of tender, organized by the National Agency for Mineral Resources of Romania in 2009. The initial participation shares of the concession holders were as follows:

- Lukoil Overseas Atash B.V. – 80%;
- Vanco International Ltd. – 20%[4].

Thus, in February 2011, a consortium with the cooperation of Lukoil concluded the concession contract with the National Agency for Mineral Resources of Romania regarding the Rapsodia and Trident perimeter[5]. Lukoil Overseas, the subsidiary of Lukoil, which handles the Trident offshore project, opened an office in Bucharest in May 2011 to manage the project. The Trident perimeter in the Black Sea has an area of 1,006 km^2 and is located at about 170 km from the shore. The water depth within the Trident perimeter

[1] Jan Kalicki, David Goldwyn, *Energy and Security: Strategies for a World in Transition*, Johns Hopkins University Press, Baltimore, 2013, p. 42

[2] Energy Analytical Studies, *EX-30 Trident – Fact Sheet*, 25.04.2024, https://energystudies.ro/ex-30-trident-fisa-descriptiva/ (27.10.2024)

[3] Benjamin Sovacool, *Energy Security*, Vol. 4, Sage Publications, London, 2013, p. 344

[4] Romgaz, *Approval of the increase of the participation share of SNGN Romgaz SA in the perimeter of exploration-development-production EX-30 Trident located in the Black Sea*, 31.01.2018, https://www.romgaz.ro/sites/default/files/2024-05/Referat%20nr.%203492%20din%2031.01.2018%20pentru%20aprobarea%20creșterii%20.pdf (27.10.2024)

[5] Reuters, *Russia's LUKOIL clinches Romania Black Sea deal*, 24.02.2011, https://www.reuters.com/article/business/-energy/russias-lukoil-clinches-romania-black-sea-deal-idUSWLB5105/ (27.10.2024)

fluctuates from 300 to 1.200 meters. According to seismic data, the area of the deposit can reach 39 km^2, and the reserves, to be confirmed by the evaluation drilling, can exceed the figure of 30 billion m^3 of natural gas[1].

Since 2011, geological exploration works have been launched in the EX-30 Trident perimeter. The works were carried out by the company Lukoil Overseas, based on the Concession Agreement concluded with the Government of Romania. In the summer of 2012, Romgaz signed a Farm-Out Agreement (acquisition) with Lukoil Overseas Atash B.V. and Vanco International Ltd. (later PanAtlantic), becoming co-owner of the exploration operations in EX-29 Rapsodia and EX-30 Trident perimeters, obtaining a 10% share of the rights and obligations of the two offshore perimeters. In 2018, following the withdrawal of PanAtlantic, Romgaz increased its participation share within the Trident perimeter. Currently, the participation share in the Concession Agreement is as follows: Romgaz - 12.2%, Lukoil - 87.8%[2]. In the early years, Lukoil focused its efforts on geological exploration and assessing the potential of gas resources. This involved exploratory drilling and detailed geological analysis.

In 2012, Lukoil began exploration in the Trident offshore perimeter. For the first time in its corporate history, Lukoil initiated upstream activities on the territory of a member state of the European Union. The company has invested in advanced technologies to meet the challenges specific to offshore activities in the Black Sea, including drilling and environmental monitoring equipment[3].

Following the drilling campaign, which took place in 2014-2015, three wells were drilled: one in block 29-Rapsodia and two in block 30-Trident. The first exploration well, Lira-1X, in the Trident block discovered a gas-saturated range of 46 meters thick with a capacity of 30 billion m^3. In 2016, following the unsatisfactory outcomes of exploration activities, Lukoil gave up the 20-Rapsodia block concession, continuing the works only on the 30-Trident block[4].

In 2017, a series of 3D seismic studies and analyses, electromagnetic surveys (EMS), as well as geochemical studies of the seabed were carried out within the Trident block. The main objective of these studies and analyses was to obtain confirmation that the gases from the Lira-1X exploration well extend over the entire area of the EX-30 Trident block. At the end of 2019, Lukoil drilled the third well within the EX-30 Trident block, the Trinity-1X well. The drilling works were carried out by the Italian company Saipem. Following the drilling of the well, several levels of natural gas-carrying formations were confirmed in the Trident perimeter. At the same time, both Lukoil and Romgaz noted that the well was a "geological success", but did not confirm the exploitation forecasts of the deposit[5]. At certain stages, Lukoil had to initiate pilot projects to test the viability of extraction technologies and methods in the Trident perimeter.

Considering the interdependence between energy (in this case natural gas) and political processes at an international level, the Trident project in its evolution has faced various challenges, including geopolitical instability in the region and fluctuations in energy prices, which have influenced investment decisions. In 2021, the management of Lukoil, at the Saint Petersburg International Economic Forum (SPIEF), stated that it is considering the possibility of supplying gas from the Trident project[6]. However, in 2023, NAMR approved Lukoil to continue the exploration program in the Trident perimeter until 2026, so the exploitation and subsequent supply of natural gas remains in question.

---

[1] Lukoil, *Project in Romania*, 20.10.2011, https://www.lukoil.com/InvestorAndShareholderCenter/RegulatoryDisclosure/-ArchiveRegulatoryDisclosure2011/20102011ReProjectinRomania (27.10.2024)

[2] Romgaz, *Approval of the increase of the participation share of SNGN Romgaz SA in the perimeter of exploration-development-production EX-30 Trident located in the Black Sea*, 31.01.2018, https://www.romgaz.ro/sites/default/files/2024-05/Referat%20nr.%203492%20din%2031.01.2018%20pentru%20aprobarea%20creșterii%20.pdf (27.10.2024)

[3] Renergy, *Energy Analytical Studies Analysis: Prospects of the offshore project EX-30 Trident in the Black Sea*, 20.05.2024, https://renergy.md/analiza-energy-analytical-studies-perspectivele-proiectului-offshore-ex-30-trident-din-marea-neagra/ (27.10.2024)

[4] Economica, *Lukoil and Romgaz have given up the Rhapsody oil perimeter in the Black Sea. No gas or oil found*, https://www.economica.net/lukoil-si-romgaz-au-renuntat-la-perimetrul-petrolier-rapsodia-din-marea-neagra-nu-au-gasit-gaz-s-au-petrol_114846.html (27.10.2024)

[5] Energy Analytical Studies, *EX-30 Trident – Fact Sheet*, 25.04.2024, https://energystudies.ro/ex-30-trident-fisa-descriptiva/ (27.10.2024)

[6] Tomas Vlcek, Martin Jirusek, *Russian Oil Enterprises in Europe. Investments and Regional Influence*, Palgrave Macmillan, London, 2020, pp. 159-160

At the same time, according to the financial reports of 2020 and 2021 (last updated by Lukoil), Romania is included in the category of states where Lukoil participates in exploration and production operations. Lukoil noted in its 2020 and 2021 financial reports that in 2019 exploration wells in the Trident perimeter were financed at 5.8 billion RUB. In its 2021 financial report, Lukoil mentions that in 2020 it had funding for its international exploration and production assets amounting to 38 billion RUB, of which 36 billion RUB were related to projects in Uzbekistan, and the other 2 billion RUB to projects in the EU, in particular Romania and Bulgaria[1]. At the same time, we can see that Lukoil is a discreet company in terms of publishing data on its upstream activities in the offshore sector of the Black Sea. Thus, we note that the data presented represents the analysis of the financial status and results of Lukoil's operations noted in its last financial reports for 2020 and 2021.

In 2020, Lukoil, due to negative results of the exploration of additional wells and in the geopolitical context of Ukraine, announced its intention to exit the Black Sea offshore project by selling the Trident concession. Nevertheless, Lukoil has not been successful in finding buyers so far. The Romanian National Agency for Mineral Resources believes that Lukoil will continue to explore the Trident offshore perimeter until 2026, taking on the associated economic risks[2].

In 2024, works were carried out to prepare the drilling of wells in the Lira 2A deposit of the Trident offshore perimeter and tenders were held to purchase drilling works, after which in April 2024 NAMR approved the participation of the partners of the association in Stage II of the optional evaluation phase[3]. Thus, the Trident project continues to evolve, but specific details about recent advances and possible natural gas discoveries vary. Lukoil continues to show interest in exploring natural resources in the Black Sea, but in a cautious form. Looking ahead, the Lira-1X well in the Trident perimeter has a production capacity of 1 – 1.5 billion m^3 of gas/year.

Prospects of the Trident offshore project

Oil and gas companies in the background of the energy transition wave have experienced a more difficult period. Government regulations and environmental policy favor companies that adopt sustainable practices. Investors are becoming increasingly concerned about the social and environmental impact of energy companies, leading oil and gas companies to adapt to attract capital[4]. Thus, Lukoil tries to streamline its processes and dispose of unprofitable assets by analyzing the costs and risks related to the development of offshore projects. As an additional restraint in this equation for Lukoil, there are also economic sanctions against Russia, adopted because of the conflict in Ukraine.

The prospects for the development of the Trident offshore project by Lukoil from our perspective are limited to the following working assumptions. Lukoil's interest in Romania's offshore sector is logical, as the company has an oil refinery (Petrotel) and a network of associated gas stations. The refinery has significant processing capacity, contributing to the production of fuels, lubricants, and other petroleum products. Therefore, the development of the Trident project would strengthen Lukoil's position in the regional energy market. Lukoil's interest in Romania is manifested through a combination of commercial strategies and investments. The company seeks to improve refining technologies and implement new sustainable gas solutions, thus responding to growing environmental requirements. In addition, Lukoil aims to expand its presence in the regional market, given the constant demand for petroleum products in Southeast Europe[5].

Against the background of the global energy transition, Lukoil is in a complex position. Although the company continues to focus on traditional extraction and refining activities, it is also investing in emerging technologies, including natural gas (the energy transition fuel), which allows it to adapt to changes in the regional energy landscape.

---

[1] Lukoil, *Financial Results*, https://www.lukoil.com/InvestorAndShareholderCenter/FinancialReports (27.10.2024)

[2] Matei Ionescu, *Lukoil has not commercially validated its gas reserves in the Trident Perimeter in the Black Sea and extends until 2026 the additional exploration campaign*, "Economedia", January 16, 2023, https://economedia.ro/lukoil-nu-si-a-validat-comercial-rezervele-de-gaze-pe-care-le-are-in-perimetrul-trident-din-marea-neagra-si-lungeste-pana-in-2026-campania-de-explorare-suplimentara.html (27.10.2024)

[3] Profit, *Romgaz continues its association with Lukoil in the Black Sea*, 21.08.2024, https://www.profit.ro/povesti-cu-profit/energie/romgaz-continua-asocierea-cu-lukoil-in-marea-neagra-21707282 (27.10.2024)

[4] David Infield, Leon Freris, *Renewable Energy in Power Systems*, John Wiley&Sons, New Jersey, 2020, pp. 21-22

[5] Rozali Plieva (Akhrieva), *Strategii rossiyskiy kompaniy na vneshnikh rynkakh*, Dashkov – K, Moskva, 2020, p. 63

Lukoil will continue the exploration program of the EX-30 Trident perimeter in the Black Sea until 2026 because like any other concessionaire in the offshore sector on the Black Sea, the company will have to periodically present a program of works and geological analyses in the Trident perimeter. Lukoil's commitment to continue the exploration program until 2026 may also reflect a favorable climate in terms of regulations and policies in Romania, which can support investments in the energy sector. Investments in exploration are often long-term. Future profits from the explorations could be anticipated by the company, which would support the program's continuation

At the same time, in addition to the favorable economic and strategic reasons, we can also mention some risks associated with the exploration of the Trident perimeter. In the context of the objective of Romania's accession to the OECD (estimating 2026[1]) and the OECD recommendations to no longer concede new natural gas exploration perimeters, for climate reasons, Trident exploration is subject to uncertain variables regarding the prospect of developing a final investment decision or marketing the project in the future[2]. Also, against the background of military operations in Ukraine and economic sanctions on Russia, Lukoil is subject to economic difficulties in the EU market[3]. Thus, Lukoil put up for sale the concession in the Trident perimeter. Possible buyers can be Romgaz (project partner of Trident) or KMG (strategic partner of Lukoil).

Lukoil's investments in exploration and offshore gas development and production potential are expected to generate a positive impact on the company's economy. In addition, because natural gas is considered as a source of energy transition, according to the EU opinion[4], the Trident project can contribute to the achievement of the climate objectives of the states in the region, and Lukoil can recover its investments from the project. In this regard, the *win-to-win* strategy can be applied. At the same time, the OECD recommendations, to which Romania has set itself the goal to adhere in 2026, regarding the non-exploration of new natural gas deposits, due to climate objectives, must be regarded by Lukoil as a last chance for the final development of the Trident offshore project and the marketing of natural gas reserves. Thus, OECD recommendations to Romania on the exploration of new natural gas deposits contribute to catalyzing decisions on the EX-30 Trident offshore project.

Offshore projects in the Black Sea represent a significant opportunity for the economic development of the region, having a considerable impact on energy security and diversification of energy sources. At the same time, the prospects for offshore projects in the Black Sea are influenced by European regulations and energy transition objectives, and the Trident project is no exception. The European Union aims to reduce carbon emissions and promote renewable energy sources, which could influence the future of traditional hydrocarbon extraction projects. However, in the current context, where energy prices are volatile and the need for secure energy resources is critical, many countries in the region believe that the development of offshore deposits remains essential.

A balanced approach, combining sustainable development with immediate energy needs, will be essential to fully harness the potential of the Trident offshore project in its operation. Another crucial aspect of the future of the project is the commitment to sustainable practices, but also the overcoming of geopolitical instability in the region. If these conditions are met, the Trident project could turn the Black Sea into a significant source of energy for the region alongside the Neptun Deep project[5], contributing to economic development and long-term energy security.

---

[1] Libertatea, *Romania aims to join the OECD in 2026, says the Government. What is the Organization for Economic Co-operation and Development*, 04.08.2024, https://www.libertatea.ro/stiri/romania-obiectiv-aderarea-ocde-oecd-2026-ce-este-ocde-oecd-4977373 (28.10.2024)

[2] OECD, *Economic Surveys Romania*, March 2024, p. 107, https://www.oecd.org/en/publications/oecd-economic-surveys-romania-2024_106b32c4-en.html (11.11.2024)

[3] Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New York, 2020, p. 20

[4] European Parliament, *Energy transition in the EU*, https://www.europarl.europa.eu/RegData/etudes/BRIE/-2023/754623/EPRS_BRI(2023)754623_EN.pdf (28.10.2024)

[5] Mihai Melintei, *The Neptun Deep Project and the Redesign of the Regional Energy Security*, "Studia Securitatis", Vol. 17, No. 2, Sibiu, 2023, p. 182

Impact of the Trident offshore project on regional energy security

Energy security is the ability of a state or a region to ensure constant, reliable and sustainable access to the energy resources necessary to support economic development and the welfare of the state. This involves not only the availability of resources, but also the diversification of energy sources, the appropriate infrastructure, price stability and protection against external threats[1].

Key aspects of energy security can be noted as follows:

- Diversification of sources: dependence on a single supplier or on one type of energy (e.g. natural gas or oil) can create vulnerabilities. States are encouraged to develop alternative sources, including renewable energy, nuclear energy or fossil fuels from various sources of supply.
- Infrastructure: A robust infrastructure including pipelines, power grids and import terminals is essential to ensure continuous energy flows. Investments in upgrading and expanding this infrastructure are crucial to prevent disruptions and ensure energy security.
- Geopolitical stability: Conflicts or political instability in the region can affect supply. Thus, energy security also depends on international relations and cooperation between states.
- Sustainability: in the context of climate change, energy security must also include the transition to cleaner energy sources. Promoting renewable energy, energy efficiency and reducing carbon emissions become key priorities.
- Energy prices: price stability is another important aspect of energy security. Sudden price fluctuations can affect economies, and countries need to develop strategies to deal with these variations[2].

As a result of the above, we can emphasize that energy security is a multidimensional field that requires an integrated approach, with collaboration between government, the private sector and civil society. By promoting diversification, upgrading infrastructure and transitioning to sustainable energy sources, states can ensure a stable and resilient energy future, able to meet economic and environmental challenges.

Concerning energy security in Southeast Europe, particularly in the Black Sea basin, this is an issue of increasing importance, given the region's geostrategy and the significant energy resources available. This area is crucial not only for the states around it, but also for Europe, considering the increased need for diversification of energy sources. In recent years, the Black Sea has become a focal point for the exploration and exploitation of natural gas. Recent gas discoveries in perimeters such as those in the Romanian area (Neptun Deep, Trident) and those off the Turkish coast (Sakarya) have attracted the attention of investors and international energy companies. These resources can help reduce the European Union's dependence on imported gas and support the transition to cleaner energy sources.

At the same time, energy security in Southeast Europe is threatened by geopolitical tensions in the region. The conflict between Russia and Ukraine, as well as the energy policies of the countries in the region on the transit of gas through Ukraine, affect regional energy stability[3]. Thus, Southeast European states must work together to develop the necessary infrastructure, such as pipelines and gas terminals, and form regional alliances that ensure constant and secure access to energy resources, such as the Vertical Gas Corridor[4].

With Black Sea gas, Southeast Europe has the potential to emerge as a local center in the gas market, playing a key role in European energy stability. By exploiting Black Sea gas, Southeast European countries can offer a viable alternative to traditional gas sources[5]. It contributes to the diversification of the European gas market and to the improvement of the energy security of the entire region[6]. In this respect, investments in offshore gas exploration, development and production in energy projects such as EX-30 Trident generate a significant impact on energy security. Here are some working assumptions for which this potential of the Trident offshore project is promising:

---

[1] Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New-York, 2020, p. 20

[2] Carlos Pascual, Jonathan Elkind, *Energy Security. Economics, Politics, Strategies, and Implications,* Brookings Institution Press, Washington D. C., 2010, pp. 51-52

[3] Energy Analytical Studies, *Perspectives of gas transit through Ukraine*, 31.05.2024, https://energystudies.ro/perspectivele-tranzitului-de-gaze-prin-ucraina/ (29.10.2024)

[4] CE Energy News, *New phase of the Vertical Corridor initiative to begin in July 2024*, 27.05.2024, https://ceenergynews.com/oil-gas/new-phase-of-the-vertical-corridor-initiative-to-begin-in-july-2024/ (29.10.2024)

[5] Rozali Plieva (Akhrieva), *Strategii rossiyskiy kompaniy na vneshnikh rynkakh*, Dashkov – K, Moskva, 2020, p. 63

[6] George Scutaru, *Black Sea's offshore energy potential and its strategic role at a regional and continental level*, "New Strategy Center", KAS, Bucharest, p. 9

- The Trident project can contribute to strengthening Romania's economic security, catalyzing the development of related economic branches (direct and indirect cumulative economic impact);
- The advancement of the Trident offshore project can contribute to the development of the region's energy-critical infrastructure as well as energy technical know-how.
- Developing a new stage in Romania's energy sector and industrial redevelopment by opening gas plants within national energy complexes (e.g. Mintia);
- With the exploration of natural gas from the Trident perimeter, they can be used for the development of renewable energy projects in the region (taking into account that natural gas is considered the fuel of energy transition);
- Trident has strong potential, fostering the development of the natural gas business environment at regional level. At the same time, the project can strengthen Lukoil's presence in the EU energy market.

Although there are several optimistic and valuable variables regarding the development of the Trident project, Lukoil has started to revise its energy strategy. In the context of geopolitical developments in the region and in response to European sanctions and other political decisions regarding its energy operations in the European Union, the company has changed its investment policies at the European level since 2023. Military tensions between Russia and Ukraine demonstrate that energy is a fundamental part of the system of international relations and new geopolitical ties[1]. Antagonism between Gazprom and Naftogaz is felt in Europe's energy markets, and Lukoil's investments and energy projects are no exception to this antagonism. As an example, the ISAB refinery in Sicily was sold by Lukoil to G.O.I. ENERGY[2], and the Rosenets port terminal in Bulgaria was transferred under state control[3], the concession to Lukoil being terminated due to sanctions[4].

In the background of military operations in Ukraine, Lukoil, as well as other Russian oil and gas companies, began to bear problems with its assets in Europe (see also the example of Gazprom in Germany[5]). Because of these significant changes in the operating conditions of its subsidiaries, Lukoil began to project new visions regarding its energy activities. In this respect, the Trident offshore project in the Black Sea is also targeted. Regarding Lukoil's oil operations in Romania, according to Kpler[6] (the global platform for commercial intelligence), now through the Caspian Pipeline Consortium (CPC) pipeline, Lukoil provides only part of the raw material needed for the Petrotel refinery in Ploiesti, the rest being provided through alternative sources. The refining capacity of the Petrotel refinery is 2.7 million tons per year, with a share of the Romanian oil market of 8-10%[7]. In the summer of 2023, Lukoil stated that "EU economic sanctions do not impose restrictions on the conduct of the company's activity under optimal conditions in Romania, but future developments and how any future restrictions may or may not influence the continuation of the company's activity in its energy projects cannot be anticipated. Now, Lukoil has not declared the sale of those 30-32 billion m^3 of natural gas in the EX-30 Trident perimeter. The Company will continue the field exploration program until 2026 with a minimum program of work. This reveals 2 hypotheses, either Lukoil wants to maintain a latent strategic position in the offshore Black Sea area, or Lukoil is looking for buyers for its assets in the Trident perimeter. At the same time, in 2024, Lukoil's total investments in field exploration are planned at the level of 47 billion RUB[8]. Although the company is not discreet in its reports on the projects where

[1] Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, NewYork, 2020, p. 20

[2] Financial Intelligence, *Lukoil sells Sicilian Refinery to G.O.I. ENERGY and Trafigura*, 09.01.2023, https://financialintelligence.ro/lukoil-vinde-rafinaria-din-sicilia-catre-g-o-i-energy-si-trafigura/ (29.10.2024)

[3] Offshore Technology, *Bulgarian Parliament Votes to end Lukoil's Concession to Operate Rosenets Oil Terminal*, 24.07.2023, https://www.offshore-technology.com/news/lukoil-rosenets-oil-terminal/ (19.10.2024)

[4] Boyko Nitzov, *Can Bulgaria Survive Without Russian Oil*, Working Paper, Center for The Study of Democracy, Sofia, 2022, p. 6

[5] Reuters, *German Regulator Takes over Gazprom Germany to Ensure Energy Supply*, 04.04.2022, https://www.reuters.com/business/energy/german-regulator-takes-over-gazprom-germania-ensure-energy-supply-2022-04-04/ (29.10.2024)

[6] Kpler, *Company*, https://www.kpler.com (30.10.2024)

[7] Eugenia Gusilov, *Key Romanian Refineries*, "COER", Issue Brief, February 2021, p. 7

[8] Interfax, *"LUKOIL" v 2024 godu uvelichit investitsii v geologorazvedku na 30%*, 04.04.2024, https://www.interfax.ru/business/954092 (30.10.2024)

exploration investments will be made, we can deduce the possible assumption that the Trident project will see an additional investment in exploration.

At the same time, as the activity of Lukoil is based to a full extent on activities of exploration, exploitation, and refining of oil, gas, or petrochemical-related products, the significant change in their prices worldwide, including CO_2 certificates (against the background of the energy transition), could significantly affect the cash flows and the fair value of the company's assets, including access to financing sources. These issues indicate that there is significant uncertainty that could significantly cast doubt on the entity's ability to continue operating in certain energy projects[1].

Currently, as previously noted, Lukoil is in the exploration phase of the EX-30 Trident perimeter. The extension of the exploration period until 2026 envisages the execution of additional reprocessing works, complex analyses, and the integration of geological and geophysical data available in the Trident offshore perimeter, to assess the potential of the discovery made and to identify possible natural gas expansions in the perimeter. Also, the extension of the exploration period allows Lukoil to outline new prospects (execution-results). This will lead to a reduction of the risks associated with the future drilling program in the Trident offshore project, as well as its exploitation.

Conclusions

Currently, about 1-2 out of 10 m^3 of gas produced in Romania comes from onshore resources, the gap from the offshore perimeter is filled by onshore production. Further development of the EX-30 Trident project can increase offshore production with a perspective of 1-1.5 billion m^3 of gas/year. Thus, the Trident project has strong potential, advancing the business environment in the natural gas sector and strengthening the presence of Lukoil in the energy market of the European Union, with the risks related to the European sanctions applied to Russia and Russian companies. At the same time, the OECD recommendations, to which Romania aims to adhere in 2026, regarding the non-exploration of new natural gas deposits, can be seen as a last chance for the development of the Trident offshore project and the marketing of natural gas reserves.

The importance of offshore gas from the Trident project for Romania is significant from several points of view.

- Energy Security: the exploitation of gas from the Trident project can contribute to increasing Romania's energy security;
- Economic Development: the natural gas extraction project can generate jobs and stimulate regional economic development, contributing to the growth of Romania's GDP;
- Investment attraction: providing a favorable framework for investments in the energy sector can attract foreign capital, which could lead to the modernization of Romania's energy infrastructure;
- Diversification of the Energy Source: Black Sea gas, in this case from the Trident project, can contribute to the diversification of Romania's energy mix, helping to better integrate into the European energy market;
- Environmental impact: it is also important to take into account the environmental impact of offshore gas exploitation, ensuring that environmental standards are respected and that negative impacts are minimized;
- Regional Collaboration: The Trident offshore project can facilitate cooperation with other countries in the region, helping to establish regional energy partnerships.

The EX-30 Trident offshore project represents a significant opportunity for Romania's development, in the context of Black Sea gas exploitation, together with the Neptun Deep project.

With the potential to contribute to energy security, and boost the local economy and industry, this project could have a positive impact on energy infrastructure. In conclusion, the offshore gas in the Black Sea, in this case, the EX-30 Trident project, represents an opportunity for Romania, but it is essential to manage it responsibly (considering Lukoil's participation in this project) and follow the principles of sustainable development.

[1] Profit, *Fate of Lukoil in Romania: all roads lead to Kazakhstan*, 12.01.2023, https://www.profit.ro/povesti-cu-profit/energie/soarta-lukoil-in-romania-toate-drumurile-duc-in-kazahstan-20978393 (30.10.2024)

Bibliography

Books

1. Infield, David; Freris, Leon, *Renewable Energy in Power Systems*, John Wiley&Sons, New Jersey, 2020
2. Kalicki, Jan; Goldwyn, David, *Energy and Security: Strategies for a World in Transition*, Johns Hopkins University Press, Baltimore, 2013
3. Pascual, Carlos; Elkind, Jonathan, *Energy Security. Economics, Politics, Strategies, and Implications*, Brookings Institution Press, Washington D. C., 2010
4. Plieva, (Akhrieva), Rozali, *Strategii rossiyskiy kompaniy na vneshnikh rynkakh*, Dashkov – K, Moskva, 2020
5. Sovacool, Benjamin, *Energy Security: Volume four*, Sage Publications, London, 2013
6. Vlcek, Tomas; Jirusek, Martin, *Russian Oil Enterprises in Europe. Investments and Regional Influence*, Palgrave Macmillan, London, 2020
7. Yergin, Daniel, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Press, New York, 2020

Articles and Studies

1. Nitzov, Boyko, *Can Bulgaria Survive Without Russian Oil*, Center for The Study of Democracy, Working Paper, Sofia, 2022
2. Gusilov, Eugenia, *Key Romanian Refineries*, "COER", Issue Brief, February 2021
3. Melintei, Mihai, *The Neptun Deep Project and the Redesign of the Regional Energy Security*, "Studia Securitatis", Vol. 17, No. 2, Sibiu, 2023
4. Scutaru, George, *Black Sea's offshore energy potential and its strategic role at a regional and continental level*, New Strategy Center, KAS, București, 2024

Documents

1. Energy Analytical Studies, *EX-30 Trident – Fișă Descriptivă*
2. European Parliament, *Energy transition in the EU*
3. Lukoil, *Financial Results: 2019, 2020*
4. OECD, *Economic Surveys Romania*, March 2024
5. Romgaz, *Aprobarea creșterii cotei de participare a SNGN Romgaz SA în perimetrul de explorare-dezvoltare-producție EX-30 Trident situat în Marea Neagră*

Web sources

1. www.ceenergynews.com
2. www.economica.net
3. www.energystudies.ro
4. www.financialintelligence.ro
5. www.interfarx.ru
6. www.kpler.com
7. www.lukoil.com
8. www.profit.ro
9. www.reuters.com
10. www.renergy.md
11. www.romgaz.ro

Akinyetun TOPE
Lagos State University of Education, Nigeria

DIGITALIZATION IN AFRICA: BETWEEN PROMOTING CIVIL RIGHTS AND STATE CENSORSHIP

Abstract:	*The spread of digital technologies in Africa has reshaped civic engagement, enabling citizens to mobilize and hold authorities accountable through online platforms. Social media platforms have become avenues for voter education and sensitization, political participation, and communication, as attested to by the recent spate of technology-based social movements. However, despite its indubitable role in promoting civil rights, digitization in Africa is caught in the web of digital authoritarianism, exemplified by state censorship. Because of its penchant for granting citizens a voice to speak to power, this empowerment has been met by significant government resistance, leading to widespread censorship and repression. This study examines the dual role of digital platforms in Africa as enablers of civic activism and instruments of state control, addressing the tension between the promotion and undermining of civil liberties through digital technology.* *This study was guided by Digital Citizenship and Panopticism and employs a qualitative approach by analyzing secondary data from policy reports, government briefs, journal articles, newspaper articles, and internet sources on digital platforms, state surveillance, and freedom of expression across sub-Saharan Africa. This study shows that while digital platforms have supported social movements and citizen rights, governments have responded with Internet shutdowns, surveillance technologies, and restrictive legislation to silence opposition.*
Keywords:	**Authoritarianism; censorship; civil rights; freedom; repression; surveillance**
Contact details of the authors:	E-mail: akinyetuntope@gmail.com
Institutional affiliation of the authors:	**Department of Political Science, College of Management and Social Sciences Education, Lagos State University of Education, Lagos State, Nigeria**
Institutions address:	Lagos State University of Education, Lagos State, 102101, Nigeria. www.lasued.edu.ng

Introduction

Africa has in the last decades witnessed remarkable growth in the adoption of technological tools in communication, education, medicine, commerce and politics. Economically, digitalization in Africa has created opportunities for economic growth by increasing opportunities for startups, entrepreneurship, and employment. For instance, an increase in mobile broadband penetration in sub-Saharan Africa has led to a 2.5% increase in Gross Domestic Product (GDP)[1]. Despite recording the lowest performance score (50.3 among the regions surveyed, 40.1 per cent of the population using the Internet and 67.0 per cent owning a mobile phone in Africa recorded a 7.8 per cent improvement in performance compared to 2023[2]. This indicates that Africa continues to make giant strides in digital transformation, while the penetration of digital tools

[1] European Investment Bank, *The Rise of Africa's Digital Economy*, European Investment Bank, Luxembourg, 2021, https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf (1.10.2024)

[2] International Telecommunication Union, *The ICT Development Index 2024*, ITU, Switzerland, 2024, https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/ (07.09.2024)

remains steady. Digitalization helps governments improve transparency and accountability by adopting e-government platforms for the deployment of basic and public delivery services[1].

The use of digital technology has been recorded in various countries' political and constitutional processes. It has enabled citizen participation in decision-making and civic engagement and has improved the quality of political participation across the board. There have been remarkable instances of the adoption of digital tools to promote civil rights in Africa. Beginning with the Arab Spring in Tunisia in 2010 and moving to the #EndSARS protests in Nigeria in 2020[2], the use of digital tools to empower social movements and demonstrations cannot be overemphasized. Digitalization creates opportunities for citizens to become deeply involved with the political system and governance through the enablement of various platforms[3]. Citizens have become better informed and empowered to express their opinions, criticize the government openly yet anonymously, vote in an election, canvass for votes, and monitor the electoral process. Digitalization has become a tool of political empowerment and an index for measuring citizen freedom, while social media platforms have become indispensable in promoting voter education, campaigns, and political indoctrination.

In addition to challenges such as the digital divide, high cost of digital access, an overwhelming illiterate population, and gender gap[4], digitalization is susceptible to perversion by authoritarian rulers for control, surveillance, and repression. The Collaboration on International ICT Policy for East and Southern Africa *(*CIPESA*)* decries the growing decline in democratic governance, deepening the digital divide, and growing digital authoritarianism in Africa[5]. Concerning the latter, authoritarian governments often adopt technology to perpetuate illegality and extend their stay in office. Governments in countries such as Mali, Chad, Burkina Faso, Algeria, Rwanda, South Sudan, Ethiopia, and Gabon have embarked on the extensive use of digital tools to limit citizen rights and freedom through media control, censorship, and internet shutdowns to spread state-centric narratives. It requires little emphasis that these disruptions limit citizen rights and undermine governance, while increasing the tendencies of despotic and authoritarian rule. However, the essence of state surveillance of its citizens is to limit opposition and enable the government to maintain a stranglehold on the state. These actions point to the larger challenge that digitalization poses to civil rights. In other words, while digitalization promotes civic activism and engagement, it also increases the risk of restricting civil rights and promoting state censorship, especially when controlled by states with authoritarian tendencies.

The above is alluded to in the Freedom in the World report 2024 which shows that 46 percent of the countries in Africa are categorized as not free 37 percent are partially free while only 17 percent are designated as free, indicating the pervasiveness of the limitations to political rights and civil liberties on the continent. Placed in context, the report further shows that 7 African countries (Niger -7; Tunisia -5; Sudan -4; Burkina Faso -3; Madagascar -3; Mali -3; and Sierra Leone -3) are among the 17 where the most significant deteriorations in political rights and civil liberties for the year 2023 were recorded[6]. This, again points to the prevailing challenge of a lack of freedom on the continent.

Social media and Internet blackouts have become trademarks of authoritarian governments such as Cameroon, Togo, and Chad in asserting control. While this is often done under the guise of sovereignty concerns and the need to preserve national security, it gives impetus to one-party authoritarian regimes to maintain their notoriety[7]. This trend is worrisome because the increase in state censorship in Africa is out of

[1] European Investment Bank, *Op. cit.*, p. 13

[2] Tope Shola Akinyetun, Victor Chukwugekwu Ebonine, *The Challenge of Democratization in Africa: From Digital Democracy to Digital Authoritarianism*, in Emilia Alaverdov, Muhammad Bari (Eds.), *Regulating Human Rights, Social Security, and Socio-Economic Structures in a Global Perspective*, IGI Global, USA, 2022, p. 260

[3] Victor Ojakorotu, *Digitalization, Politics, and Governance in Africa*, "E-Journal of Humanities, Arts and Social Sciences", Vol. 1–2, 2023, p. 4

[4] Kashema Bahago, Adedeji Adeniran, Uchenna Efobi, *The Role of Digitalisation in Inclusive Governance: A Case Study of Sub-Saharan Africa (Occasional Paper No. 79)*, "Southern Voice", 2023, http://southernvoice.org/wp-content/uploads/2023/04/Digitalisation-sub-Saharan-Africa-Bahago-Adeniran-Efobi-2023.pdf (1.10.2024)

[5] CIPESA, *State of Internet Freedom in Africa 2024: Africa's Electoral Democracy and Technology*, 2024, https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf (1.10.2024)

[6] Freedom House, *The Mounting Damage of Flawed Elections and Armed Conflict*, Freedom House, Washington DC, 2024, https://freedomhouse.org/sites/default/files/2024-02/FIW_2024_DigitalBooklet.pdf (1.10.2024)

[7] Amodani Gariba, *Enter the Dragon: The Impact of China's Digital Authoritarianism on Democracy in Africa*, "The Africa Governance Papers", Vol. 1, No. 4, 2023, p. 41, https://tagp.gga.org/index.php/system/article/view/53 (07.09.2024)

the playbook of China. China remains one of the largest economic partners of African countries and has systematically exported surveillance and censorship technologies to encourage states with authoritarian ambitions. This not only emphasizes the role of external countries in promoting digital abuse and censorship in Africa, but also raises a bigger question of Africa's digital sovereignty and overall Internet freedom. This is particularly worrying for a continent like Africa, which depends on foreign countries for the development of its digital infrastructure. Further, in context, data from the Ibrahim Index of African Governance show that digital freedom in Africa between 2014 and 2023 experienced significant decline. A comparison of the regions in Africa shows that each region recorded a decline in digital freedom, especially Northern Africa, where a decline of -9.2 was recorded, followed by Western Africa with a -9.0 decline (see Figure 1). Concerning West Africa, aside from Gambia, other states in the region recorded a downward trend in digital freedom between 2014 and 2023 with Senegal being the most challenged, having recorded -27.3 over the period of review (see Figure 2). The figures show the extent of decline in digital freedom in Africa.

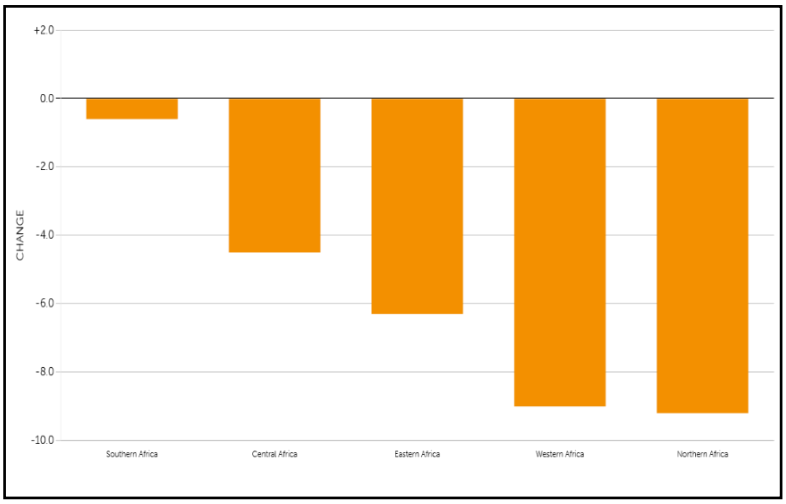

Figure 1. Digital Freedom for Africa (2014-2023)[1]

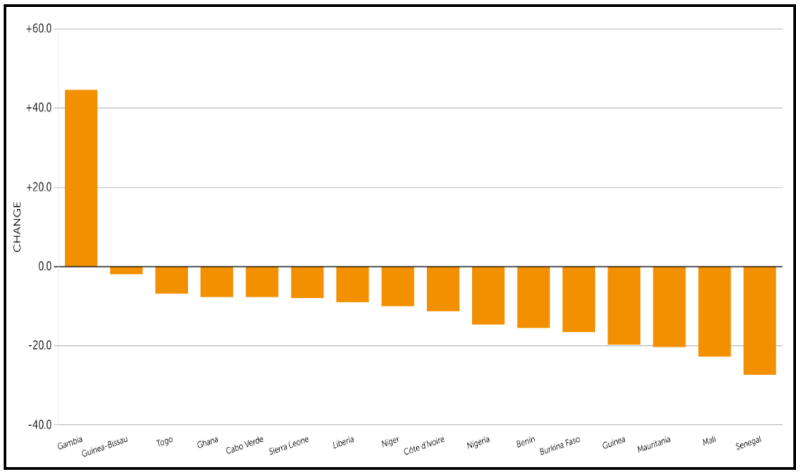

Figure 2. Digital Freedom for West Africa (2014-2023)[2]

Theoretical perspectives

Digital citizenship

Citizenship has evolved in contemporary times from the traditional notion of having duties and responsibilities to the state to promoting a virtual community where individuals are empowered to contribute to

[1] IIAG, *Digital Freedom in Africa*, 2024, https://iiag.online/data (1.10.2024)
[2] *Idem*

political life, participate in democracy and influence decision making outside the norm[1]. The concept of citizenship allows an individual to lay claims for social, political, and civil rights. Social rights include economic welfare, security, and education, while political rights include membership in a political authority and the ability to participate in political and democratic systems, including the electoral process. Civil rights include those that guarantee freedom of speech, right to own property, and right to justice. Given that citizens require unfettered information to make decisions and participate in politics, Internet access thus becomes a social, political, and civil right[2]. Viewed as a right, Internet access enables citizenship and affords citizens the opportunity to use various platforms to gain and disseminate information, thus conferring on them the status of digital citizenship. Digital citizenship hinges on three ideas: involvement in the digital space, making use of opportunities to develop the digital space, upholding civic rights, and holding government accountable through digital technologies. Digital citizenship is crucial for collective resilience, security, and mobilization[3].

Digital citizenship refers to the ability of citizens to gain access to the Internet and participate effectively in society. This emphasizes how the Internet and digital technological tools empower citizens, enhance their civil rights, and enable them to function adequately. At its core, the idea underscores access to the Internet as a precondition for full citizenship, social justice, equality of opportunities, and as a notable requisite for effective democracy and civic participation[4]. The concept is hinged on three components: "constant questioning of the policies of all nations, active interest in the affairs of other countries, and an interest in creating a just global order"[5]. Digital citizenship refers to the adoption of mobile and digital tools to participate in political and civic life online. It is acquired by using technology tools in social and political interactions without necessarily partaking in formal politics[6]. This makes participation possible for citizens through access to information on political matters. With this, citizens are empowered to evaluate government actions and demand transparency while maintaining the responsibility of improved communication[7].

The study of digital citizenship witnessed a pivotal moment with the Cambridge Analytica scandal and Snowden revelations, which revealed how private corporations and state governments used social media platforms such as Facebook for the surveillance of citizens and manipulated voting behavior. As the Snowden revelation showed, liberal and authoritarian governments engaged in mass surveillance of citizens to manipulate the electoral process and impinge on citizen civil rights[8]. A digital citizen possesses cognitive, affective, and psychomotor skills to use technological tools to communicate, create information, and influence policy. That is, digital citizens are technologically literate, embedded in the prevalent global digital culture, possess a deep understanding of the Internet, are aware of digital communication laws, possess moral obligation to communicate using digital tools, are active social media users, are aware of debates on digital privacy, and support participatory democracy[9]. Generally, digital citizens engage in multifaceted

---

[1] Şevki Işıklı, *Digital Citizenship: An Actual Contribution to Theory of Participatory Democracy*, "AJIT-e: Online Academic Journal of Information Technology", Vol. 6, 2015, pp. 21-37, https://doi.org/10.5824/1309-1581.2015.1.002.x (07.09.2024)

[2] Toks Dele Oyedemi, *Internet Access as Citizen's Right? Citizenship in the Digital Age*, "Citizenship Studies", Vol. 19, No. 3–4, 2015, pp. 450-464, http://dx.doi.org/10.1080/13621025.2014.970441, (10.08.2024)

[3] Ayobami Ojebode, Babatunde Ojebuyi, Oyewole Oladapo, Marjoke Oosterom, *Ethno-Religious Citizenship in Nigeria: Ethno-Religious Fault Lines and the Truncation of Collective Resilience of Digital Citizens: The Cases of #ENDSARS and #PantamiMustGo in Nigeria*, in Tony Roberts, Tanja Bosch (Eds.), *Digital Citizenship in Africa: Technologies of Agency and Repression*, Zed Books, New York, 2023, p. 112, https://library.oapen.org/handle/20.500.12657/63749 (17.11.2024)

[4] Toks Dele Oyedemi, *The Theory of Digital Citizenship*, in Jan Servaes (Ed.), *Handbook of Communication for Development and Social Change*, Springer, Singapore, 2020, p.15, https://doi.org/10.1007/978-981-10-7035-8_124-1 (17.11.2024)

[5] Cristina Hennig Manzuoli, Ana Vargas Sánchez, Erika Duque Bedoya, *Digital Citizenship: A Theoretical Review of the Concept and Trends*, "Turkish Online Journal of Educational Technology", Vol. 18, 2019, pp. 13-14

[6] Tony Roberts, Tanja Bosch, *Spaces of Digital Citizenship in Africa*, in Tony Roberts, Tanja Bosch (Eds.), Digital Citizenship in Africa: Technologies of Agency and Repression, Zed Books, New York, 2023, p. 7, https://library.oapen.org/handle/20.500.12657/63749 (17.11.2024)

[7] Cristina Hennig Manzuoli, Ana Vargas Sánchez, Erika Duque Bedoya, *Op. cit.*, p. 16

[8] Tony Roberts, Tanja Bosch, *Op. cit.*, p. 10

[9] Işıklı, Şevki, *Digital Citizenship: An Actual Contribution to Theory of Participatory Democracy*, "AJIT-e: Online Academic Journal of Information Technology", Vol. 6, 2015, p. 22, https://doi.org/10.5824/1309-1581.2015.1.002.X, (10.08.2024)

communication, gathering and dispersing information rapidly, acting as critiques of government policies, engaging in social media gossip, and striving for digital equality[1]. Despite its strengths, the idea has been criticized as entrenching inequality, as it widens the digital divide between technologically savvy and those who are not, and between urban and rural areas, especially in economically disadvantaged countries[2].

Panopticism

The concept of Panopticon traces its origin to Jeremy Bentham and was popularized by Michel Foucault in his book Discipline and Punish. The idea was conceived as a prison architectural design to watch prisoners without knowing that they were being watched. This is a way of internalizing control, such that the prisoner is his own guard. This refers to the change in behavior occasioned by surveillance[3,4]. Bentham's panopticon which symbolizes a prison that allows for an all-seeing entity to act as an inspector over inmates without being seen forces inmates to adjust their behavior considering the possibility that they may be watched. The prison is aimed at producing self-discipline and restraint as inmates are forced to be cautious knowing that they may be under surveillance[5]. Manokha identifies three assumptions of the concept: an omnipresent and invisible inspector; visible objects of surveillance; and the assumption of being watched[6]. Wrobel asserts that "there are five levels of surveillance inside Bentham's project: the prisoners are watched by the authorities, the governor watches the wards, the wards watch the governor, the inmates watch each other, and the whole structure is open to the public"[7]. The use of panopticons in surveillance studies refers to the idea that states and business corporations act as watchers to acquire power over and control the watched. This describes the improved capability of watchers to invade the privacy of citizens and maintain domination through surveillance technology. It is seen as an efficient form of power and structure of domination imposed to control individuals who lack the power to resist[8]. Surveillance is defined as a systematic process of vigilance to collect personal details to influence the subject[9]. The metaphor of panopticon interacts closely with modern surveillance, where individuals become conscious of the data they put out, knowing that such data may be gathered and stored by the government to exercise control over them[10]. This, no doubt, has grave implications for individual rights, as their privacy is not only subject to external interference, but they must constantly watch over their shoulders to ensure that they are subjects of surveillance or censorship.

This is more troubling considering the proliferation of digital technology and its adoption in everyday use. The implication is that citizens' civil rights, freedom of expression, and social mobilization suffer from double jeopardy, self-censorship, and state or corporate surveillance[11]. This undermines participatory democracy, increases the risk of state repression, and continues authoritarianism. With the increase in breaches of privacy on social media evidenced in the Facebook/Cambridge Analytica scandal, the susceptibility of digital technology and social space to surveillance, and the risk it poses to its users[12]. The resulting digital traces from the digital actions undertaken over the Internet, such as tweets and mobile calls, enable authoritarian states to engage in state censorship, surveillance, manipulation, and control of citizens, thus limiting civic engagement[13].

Foucault's culture of surveillance has become a culture among big corporations that are often locked in a race of control and are moved by economic benefits, as well as by state governments with authoritarian

---

[1] *Idem*
[2] Cristina Hennig Manzuoli, Ana Vargas Sánchez, Erika Duque Bedoya, *Op. Cit.*, p. 17
[3] Mark Rathbone, *Panopticism, Impartial Spectator and Digital Technology*, "The Indo-Pacific Journal of Phenomenology", Vol. 22, No. 1, 2022, p. 1
[4] Claire Wrobel, *Introduction: Literary and Critical Approaches to Panopticism*, "Revue d'études Benthamiennes", Vol. 22, 2022, p.1
[5] Ivan Manokha, *Surveillance, Panopticism, and Self-Discipline in the Digital Age*, "Surveillance & Society", Vol. 16, No. 2, 2018, pp. 219–237, https://doi.org/10.24908/ss.v16i2.8346 (01.09.2024)
[6] *Idem*
[7] Claire Wrobel, *Op. cit*., pp. 2-4
[8] Ivan Manokha, *Op. cit*, p. 221
[9] David Lyon, *Surveillance*, "Internet Policy Review", Vol. 11, No. 4, 2022, p. 14
[10] Ivan Manokha, *Op. cit*., p. 226
[11] *Ibidem*, p. 232
[12] Mark Rathbone, *Op. cit.*, p. 1
[13] Tony Roberts, *Op. cit.*, p. 12

orientation[1]. Meanwhile, surveillance itself has become a capitalist venture that big corporations embark upon to guarantee a surplus. Surveillance capitalism "is a new form of capitalism that uses advances in digital technology to survey personal and relationship spaces under the guise of 'deep support,' to be turned into cash"[2]. Foucault's notion of a panoptic gaze – dominant forms of mental control that state exercises on citizens – explains the gatekeeper state prevalent in Africa where the state engages in intrusive and unobtrusive surveillance and social control[3]. While the use of digital technology has afforded its users the ability of inverse gaze by using mobile phones and social media platforms to monitor government actions, their digital footprints in cyberspace often give away too much information about them. That is, while citizens have organized themselves as digital dissidents to engage in political conversations and liberation struggles, their vulnerability to state surveillance increases the chances of intimidation and harassment[4].

Digital platforms and civil rights

The use of digital technologies for the interaction and sharing of texts, images, and videos has become popular among African citizens. This has enhanced their ability to organize themselves in support of or against the government[5]. The use of social media platforms and hashtags is essential for driving critical discourse. They constitute avenues for critiquing government policy, demanding justice, and campaigning for good governance. Viral hashtags have been used in Nigeria to address specific governance and socio-political issues. These include #BringbackOurGirls, #SaveNigeriaGroup (SNG), #OccupyNigeria, #ArewaMeToo, #OccupyNASS, #EndSARS, and #OurMumuDonDo. The #EndSARS remains one of the most pivotal avenues of the Nigerian populace to criticize police brutality and demand for good governance. The protests, which lasted for several days began as online expressions and quickly spread into demonstrations. This demonstrates the power of digital space and its role in solidifying interests[6]. Digital tools have evolved as tools for youth activism, civic engagement, and social movements around Africa. Popular among these are #FreeSenegal, #Zimbabweanlivesmatter, #Shutitalldown, #FeesMustFall, #EndSARS, #Congoisbleeding. This growing Internet freedom has attracted opposition from the government, leading to the latter responding through censorship, surveillance, Internet tax, Internet shutdown, and social media bans[7].

Hashtag	Description and Focus	Source
#FreeSenegal	Protests following the government's limiting access to the Internet and restricting access to social media platforms on June 1, 2023. The government sought to implement a daily curfew on Internet shutdowns. The government claimed that this was necessary to prevent the spread of hateful and subversive messages that constituted public disturbance. People resorting to using virtual private networks (VPN) to circumvent the blockage and raise awareness of issues on Twitter.	Government Technology
#Zimbabweanlivesmatter	This campaign was against President Emmerson Mnangagwa's human rights abuse and violations. The Zimbabwean president arrested over 60 protesters against government corruption and human rights abuse on July 31, 2020. The government was also accused of suppressing political opposition, journalists, and ordinary citizens as well as abducting activists, including Josphat Mzaca Ngulube. As a result, citizens took social media to tweet the abuse. This gained momentum when celebrities such as Ice Cube retweeted the messages.	France 24
#Shutitalldown	This was promoted by demonstrators, predominantly women, against gender-	Civicus

[1] Mark Rathbone, *Op. cit.*, p. 1
[2] *Ibidem*, p. 7
[3] Farooq Kperogi, *Introduction*, in *Digital Dissidence and Social Media Censorship in Africa*, Routledge, New York, 2022, p. 8
[4] *Ibidem*, p. 10
[5] Tony Roberts, Tanja Bosch, *Op. cit.*, p. 14
[6] Victoria Ibezim-Ohaeri, Joshua Olufemi, Lotanna Nwodo, Oluseyi Olufemi, Ngozi Juba-Nwosu, *Security Playbook of Digital Authoritarianism in Nigeria*, "Action Group on Free Civic Space", 2021, https://closingspaces.org/download/7808/?tmstv=1730893658 (01.10.2024)
[7] Tope Shola Akinyetun, *State of Democracy in Africa: Democratic Decline or Autocracy?*, "Političke Perspektive", Vol. 12, No. 2, 2022, pp. 89–115, https://doi.org/10.20901/pp.12.2.04 (10.08.2024)

	based violence, rape culture, and protection of the rights of the vulnerable in Namibia. This was necessitated by the search for a 22-year-old girl Shannon Wasserfall, whose body was found by the police in a shallow grave. As a result, protesters called on the president to declare a state of emergency against rising femicide and gender-based violence in the country, prompting #shutitalldown. The protestors were attacked by the security agents and subsequently dispersed	
#FeesMustFall	This captures South African students' protests the costs of tertiary education in the country on October 14, 2016. The protests began after the University of Witwatersrand announced a 10.5% increase in tuition fees. The protests quickly spread to other institutions as students in Cape Town joined. This led to disruptions in the school program, while the protests turned violent on October 21, attracting force from security agencies.	Global Citizen
#EndSARS	The Special Anti-Robbery Squad (SARS) was an investigative arm of the Nigerian Police saddled with combatting armed robbery and such other vices. Due to its success in the southern part of the country, squad operations were introduced in other parts of the country. However, given limited oversight and operational deficiencies, the squad deviated from its mandate and began to engage in extra-judicial activities, such as harassment, rape, extortion, unlawful arrest, intimidation, and other vices. It was also accused of engaging in abduction and disappearance, while uncharacteristically profiling young men and lebelling them fraudsters and cybercriminals. After years of accusations and the inability of the Nigerian government to curtail squad activities, Segun Awosanya raised a call for its disbandment in 2017. However, the squad continued its extra-legal activities unperturbed until a video showing members of the squad killing a young man went viral on th e social media. As a result, Nigerian youth mobilized on social media platforms and took to the streets to demonstrate against the squad and the government. These nationwide protests that took place in 2021 began to gain serious momentum from within and outside the country and from notable celebrities, forcing the government to clamp down on the protesters leading the death and injury of many.	Akinyetun (2021)
#Congoisbleeding	This campaign was used to decrease the level of resource exploitation and genocidal killing in the DR Congo. It is believed that the exploitation of the country's natural resources, such as cobalt used in producing batteries from mobile phones, has not translated to development; rather, it has increased the incidence of economic exploitation and wanton killings; hence, the saying Congo is bleeding. In addition to the exploitation and brutal killings from years of colonial rule, the country has recorded killings of over six million people since 1996. As a result, citizens have taken social media platforms to call attention to the situation in the country by 2023.	Tan Tv Studios
#FixTheCountry	This captures the demands of Ghana youth for improved living conditions. Social media users in 2021 used this movement to campaign for education and jobs, reduce taxes, and discourage corruption. In response, a member of parliament sponsored the #FixYourSelf campaign asking the youth to fix themselves before asking the same from the government.	DW

Table 1. Hashtags for Promoting Civil Rights in Africa[1]

The campaigns captured above point to the use of social media platforms and digital technologies to advocate human rights and civil liberties. As shown above, the tools have been used to draw attention to various matters, including Internet shutdown, human rights violations, civil rights abuses by the government, demand for gender equality, demand for student rights, protests police brutality, protests exploitation, and demands for improvement in living conditions. This underscores the notion that there is no limit to the extent to which digital technologies promote civil rights and liberties. However, despite its merits, these tools have also become instruments of repression by governments of the world, including Africa. For instance, the government in Nigeria has engaged in different tactics to criminalize and silence digital rights, tagging it a threat to national security. For instance, activists have been arrested and jailed to criticize the government on

[1] Tope Shola Akinyetun, *Reign of Terror: A Review of Police Brutality on Nigerian Youth by the Special Anti-Robbery Squad*, "African Security Review", Vol. 30, No. 3, 2021, pp. 368–385, https://doi.org/10.1080/10246029.2021.1947863 (10.08.2024)

Twitter (now X) and Facebook[1]. A case in point is the arrest of an anonymous whistleblower referred to as PIDOM known for posting materials critical of the government on X. PIDOM, allegedly named Bristol Isaac Tamunobiefiri, who was accused by the Nigerian government of leaking classified documents, undermining the government, unlawful possession, and cybercrime-related offences, was arrested on August 5 in Rivers State by the Nigeria Police Force National Cybercrime Center[2]. His arrest not only represents a significant threat to digital rights and civil liberties but also increases the chances of self-censorship[3].

Digital authoritarianism and state censorship in Africa

Owing to the popularity of the Internet and its adoption in communication and knowledge sharing, it has evolved as an efficient tool in policy and decision-making. As a result, digital tools have come under attack and are hijacked by illiberal regimes to control their citizens. This is done using a specific or combination of tactics, such as Internet shutdown, surveillance and monitoring, and censorship. This section discusses the incidence of these strategies in Africa. However, to understand this phenomenon, it is essential to conceptualize digital authoritarianism (DA). Akinyetun and Ebonine described DA as a perversion of the Internet and digital tools by authoritarian leaders to suppress civil liberty and entrench political control. In addition to being anti-democratic, this practice reduces citizens' trust in the use of digital technologies for fear of privacy invasion and repression[4]. In other words, DA emphasizes the negative uses of digital tools and how they have risen to become tools of state censorship to promote civil rights. To buttress, we analyze data from the Ibrahim Index of African Governance, which shows the level of change in digital freedom in Africa from 2014 to 2023 (see Figure 3). The data confirms that while digital freedom has experienced both positive (13 countries) and negative (41 countries) changes within the time frame, a majority of the countries in Africa have recorded a decline in digital freedom, particularly in Senegal (-27.3), Mali (22.7), Tanzania (-22.5), Mauritius (-21.7), Mauritania (-20.3), Guinea (-19.7), Gabon (-19.5), Djibouti (-17.0) and Burkina Faso (-16.5). Digital freedom here refers to sub-indicators such as freedom of expression online, absence of Internet and social media shutdowns, unrestricted access to Internet content, and Internet users' privacy protection[5]. The tools of digital authoritarianism include surveillance, social and electoral manipulation, censorship and cyberattacks, and espionage[6].

[1] Socio-Economic Rights and Accountability Project (SERAP), *Crackdown on Media Freedom and Civic Space in Nigeria*, SERAP, Lagos, 2024, pp. 32, https://serap-nigeria.org/2024/04/06/download-crackdown-on-media-freedom-and-civic-space-in-nigeria/ (07.09.2024)

[2] Solomon Odeniyi, *Anonymous Whistleblower, PIDOMNigeria, Arrested for Leaking Classified Documents, Others – Police*, "Punch", August 24, 2024, https://punchng.com/anonymous-whistleblower-pidomnigeria-arrested-for-leaking-classified-documents-others-police/ (01.10.2024)

[3] Victoria Ibezim-Ohaeri, Joshua Olufemi, *Op. cit.*, p. 52

[4] Tope Shola Akinyetun, Victor Chukwugekwu Ebonine, *Op. cit*., p. 254

[5] IIAG, *Op. cit.*, p. 1

[6] Tope Shola Akinyetun, *Democratic Backsliding in Africa: Understanding the Current Challenges*, "Kujenga Amani", Social Science Research Council, Brooklyn, 2022, p. 2, https://kujenga-amani.ssrc.org/2022/09/20/democratic-backsliding-in-africa-understanding-the-current-challenges/ (07.09.2024)

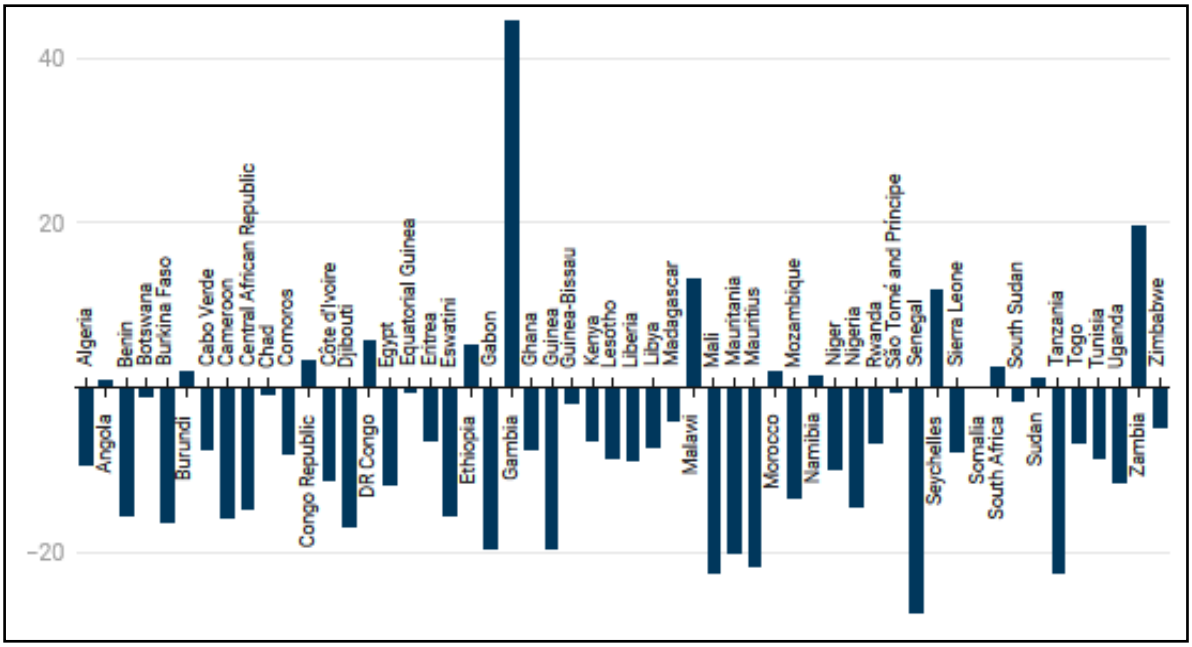

Figure 3. Digital Freedom in Africa: 2014 – 2023[1]

One of the most popular methods of restricting digital rights in Africa is through internet shutdown. Internet shutdown refers to a break in communication owing to the intentional disruption of connectivity networks. It is often carried out by Internet companies for maintenance purposes and by governments to restrict citizen information flow in flagrant violations of citizen freedom of expression. Internet shutdown places severe strains on digital citizenship, as citizens are denied the right to use mobile phones and social media platforms to express themselves and join associations of choice[2]. Meanwhile, Internet shutdowns are not unique to Africa. Available data shows that Africa is one of the least affected regions with respect to this phenomenon. The data show that Internet shutdown is more prevalent in the Asia Pacific, Middle East, North Africa, and Eastern European regions compared to Africa (see Figure 4).

[1] IIAG, *Op.Cit..*, p. 1

[2] Felicia Anthonio, Tony Roberts, *Internet Shutdowns and Digital Citizenship*, in Tony Roberts, Tanja Bosch (Eds.), *Digital Citizenship in Africa: Technologies of Agency and Repression*, Zed Books, New York, 2023, p. 211, https://library.oapen.org/handle/20.500.12657/63749 (07.09.2024)

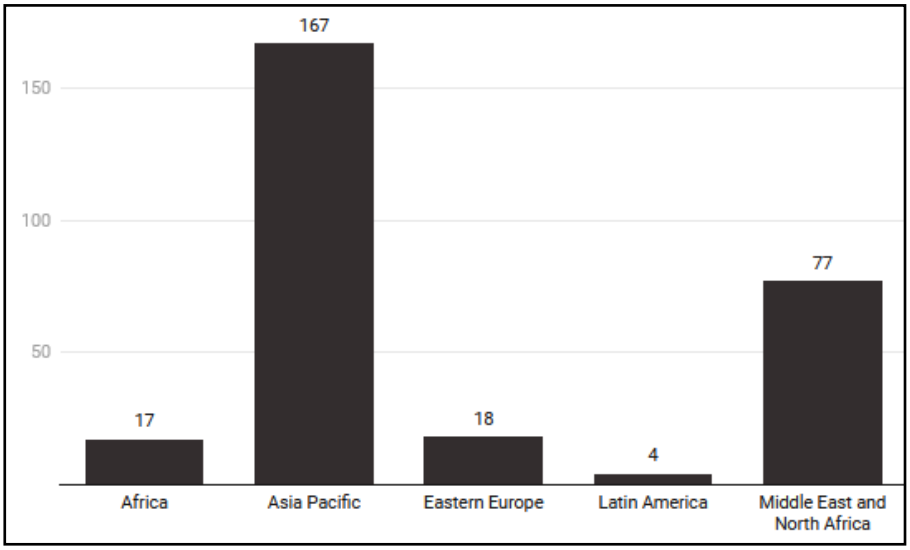

Figure 4. Internet Shutdown by Region[1]

Internet shutdowns have been recorded in various parts of the world over the past few years. Available data show that since 2016, there have been documented cases of Internet shutdowns with incidence ranging from as low as 23 to as high as 40 in a year (see Figure 5). This is further evidence that the phenomenon is not an African problem, and neither was it generated from the continent. However, it has become prevalent in Africa in recent times, as authoritarian regimes seek to elongate their stay in office and guarantee sit-tightism. For instance, between 2021 and 2023, 45 cases of internet shutdown were recorded in 28 countries (see Figure 6).

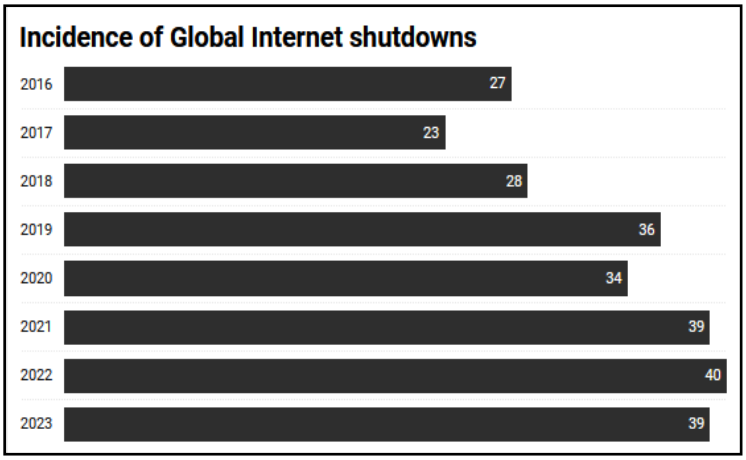

Figure 5. Incidence of Global Internet Shutdown, 2016-2023[2]

[1] Zach Rosson, Felicia Anthonio, Carolyn Tackett, *Shrinking Democracy, Growing Violence*, "Access Now", 2024, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf, (01.10.2024)
[2] *Idem*

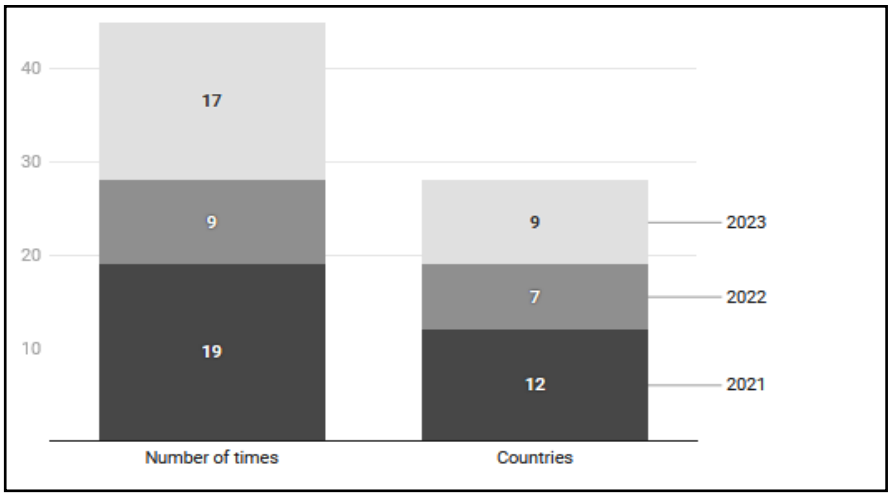

Figure 6. Internet Shutdown in Africa, 2021-2023[1]

Internet shutdown in Africa was traceable to the Arab Spring in the 2010s, when digital services were interrupted in Egypt, Tunisia, and Libya to curtail the spread of protests. Meanwhile, the DR Congo disrupted its Internet services ahead of the elections in 2011. Given the success of Internet shutdown and digital services disruption in these countries, the phenomenon has become frequent in Africa, where governments disrupt services at will for electoral purposes or to clamp down on opposition and dissidents[2]. Internet shutdowns are often severe during election periods. This trend has been recorded in Zimbabwe, Sierra Leone, Libya, South Sudan, Gabon, and Sudan. It is often aimed at restricting civic activities by limiting access to digital platforms. For instance, Ethiopia experienced the longest shutdown, spanning over 1,153 days, on November 4, 2020[3]. The Zimbabwean government shut down the Internet between January 2019 and July 2020 to curtail citizen agitation against an increase in fuel prices. Meanwhile, the Nigerian government under President Buhari placed a ban on Twitter (X) in 2022 because the president's tweet about the Nigerian Civil War, which took place between 1967 and 1970, was deleted. However, in Sudan, the government shut down the Internet in October 2021 and June 2022 following military putschism in the country[4]. Internet shutdowns were recorded in Sudan in December 2019, February 2019, June 3 – July 9, 2019, May 14 – May 16, 2020, September 13, 2020 – September 24, 2020, June 19, 2021 – June 30, 2021, and October 25, 2021 – November 18, 2021[5].

Data from Net Blocks show that the military regime in Sudan employs a variety of techniques such as telecommunications blackouts, social media, and network restrictions[6]. Internet shutdowns have political and economic effects. In addition to negating its commitment to the digital sector, Internet shutdown has cost African countries $3.9 billion (USD). While 22 countries have experienced Internet shutdowns between 2020 and 2024, the largest offenders and economic losers in the continent include Nigeria ($1,500 million), Ethiopia ($1,020 million), Algeria ($762 million), Sudan ($257 million), and Senegal ($120 million)[7]. In addition, shutdowns limit the operation of charitable activities in the region, escalating humanitarian needs in the respective countries, and undermining citizen rights. For instance, in Sudane, limited access to Internet services increased the incidence of hunger, scarcity, and poverty. While this is partly attributable to the

[1] *Idem*

[2] Tope Shola Akinyetun, Victor Chukwugekwu Ebonine, *Digital Democracy and Democratic Decline: Unpacking the Role of Digitalization in Undermining Democracy in Africa*, "African Journal of Democracy and Election Research", Vol. 3, No. 1, 2023, p. 161

[3] Gbenga Sesan, *How Africans Can Prepare for Internet Shutdowns*, "Carnegie Endowment", April 25, 2023, https://carnegieendowment.org/posts/2023/04/how-africans-can-prepare-for-internet-shutdowns?lang=en (07.09.2024)

[4] Zach Rosson, Felicia Anthonio, Carolyn Tackett, *Op. cit.*, p. 1

[5] CIPESA, *Sudan's Bad Laws, Internet Censorship and Repressed Civil Liberties*, 2021, https://cipesa.org/wp-content/files/briefs/Sudans_Bad_Laws_Internet_Censorship_and_Repressed_Civil_Liberties_2021.pdf (01.10.2024)

[6] Net Blocks, *Internet Disrupted in Sudan Amid Protests Against Military Junta*, June 30, 2022, https://netblocks.org/reports/internet-disrupted-in-sudan-amid-protests-against-military-junta-QAdPrkAl, (07.09.2024)

[7] Jasmine Ikorougo, Ujunwa Umeokeke, *Digital Self-Sabotage: The Cost of Internet Shutdowns in Africa*, "Africa Practice", 2023, https://africapractice.com/digital-self-sabotage-the-cost-of-internet-shutdowns-in-africa/ (01.10.2024)

ongoing civil war in the country, the lack of communication between humanitarian volunteers due to Internet shutdown stalled the delivery of goods and services to the affected regions and made it impossible to report atrocities in conflict-prone zones[1].

State surveillance is pervasive in Africa, especially in countries such as Gabon, Malawi, Equatorial Guinea, Senegal, Chad, Zimbabwe, Ghana, South Africa, the Democratic Republic of Congo (DRC), Nigeria, Cameroon, and Congo[2]. Surveillance refers to the observation and monitoring of individuals over a certain period. Once this is carried out by state agencies, it becomes state surveillance. African governments have expended much on surveillance technologies[3]. The governments of Ghana, Zambia, Malawi, Morocco, and Nigeria collectively spend an estimated US$1 billion a year to procure tools from Israel, China, the UK, and the EU. Despite this humongous cost, these countries have focused on different aspects of surveillance. Expanding hundreds of millions of dollars on surveillance tools, Nigeria spends the most patronizing various companies on acquiring car number plates and facial recognition. Morocco focuses on acquiring CCTV cameras from Chinese companies, Morocco favors mobile phone interception, Ghana spends heavily on mobile phone spyware, and Zambia invests in safe city surveillance.

These countries have jointly tracked and arrested regular citizens, activists, and journalists[4]. According to the International Press Institute, journalists are one of the victims of surveillance and censorship in Africa, especially in Burkina Faso, Kenya, Sudan, and DR Congo[5]. Available data shows that journalists are some of the most obvious victims of media repression in Africa. Incidents of arbitrary arrests, censorship, attacks, and restrictions on information involving journalists have been recorded in various African countries, including Burkina Faso, Kenya, Sudan, and DR Congo (see Figures 7 and 8). This is primarily sponsored by state actors, particularly state security, regulatory bodies, and government officials. With respect to Sudan, four journalists including Allaaddin Ali Mohamed, Muawiya Abdel Razek, Ibrahim Abdullah and Makawi Mohamed Ahmed were killed in Sudan.

6

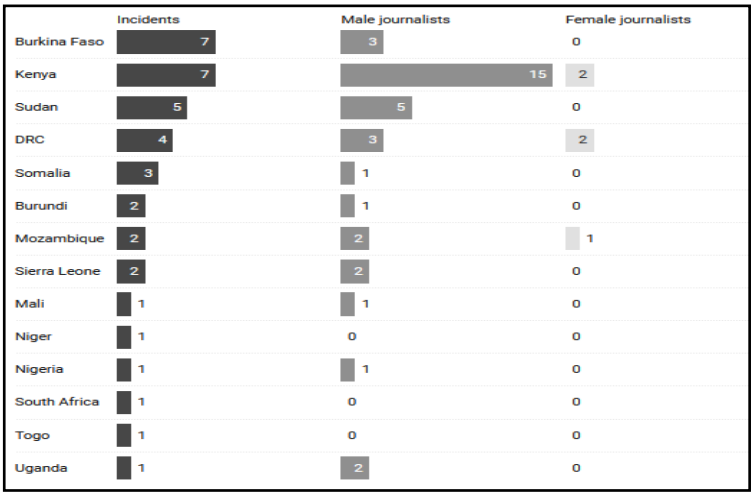

Figure 7. Media Repression involving Journalists

[1] Khanyi Mlaba, *Africa's Internet Shutdowns: Where, Why, and How Do They Happen?*, "Global Citizen", May 9, 2024, https://www.globalcitizen.org/en/content/africa-internet-shutdowns-impact-human-rights/ (01.10.2024)

[2] Mugambi Laibuta, Kuda Hove, Ridwan Oloyede, Aishat Salami, *The State of Deployment of Surveillance Technologies in Africa*, "Paradigm Initiative", 2024, https://paradigmhq.org/wp-content/uploads/2024/05/The-state-of-Digital-Surveilance-1.pdf (07.09.2024)

[3] *Idem*

[4] Tony Roberts, *Op. Cit.*, p. 12

[5] International Press Institute, *Press Freedom Violations in Africa*, IPI, 2024, https://ipi.media/wp-content/uploads/2024/07/africa-factsheet-june-2024.pdf (01.10.2024)

[6] *Idem*

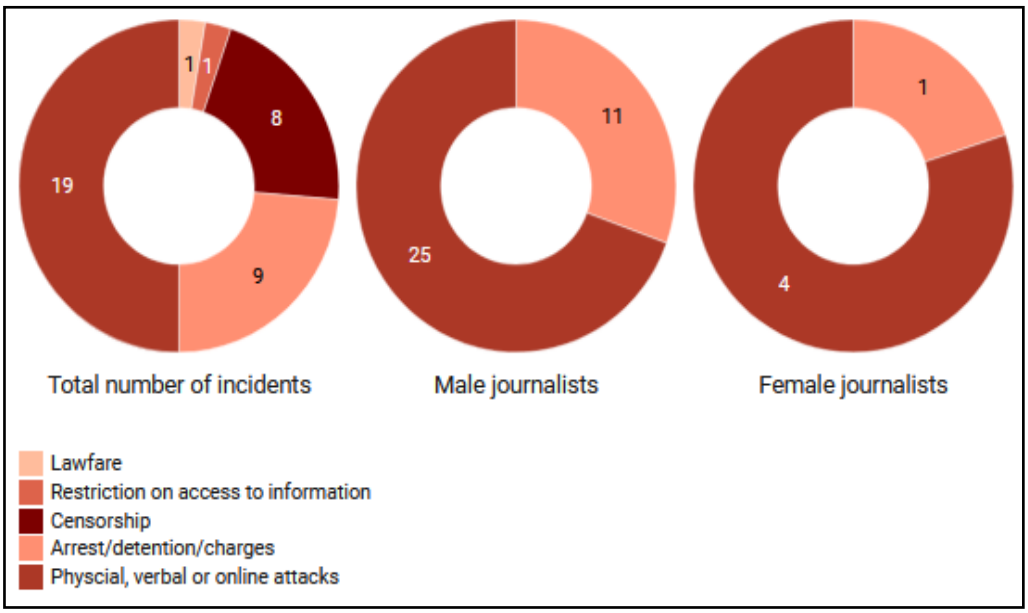

Figure 8. Forms of Attack on Journalists[1]

Governments also engage in website blocking, censorship, and the use of legislation to repress citizens. These are either couched as cybercrime laws or counterterrorism laws designed to arrest dissidents and opposition. This is evident in Bahrain, where questionable tweets attract jail sentences. Meanwhile, authoritarian regimes, such as those in the Arab world, continue to invest in surveillance technologies to spy on citizens and maintain control over them[2]. Using Egypt, Palestine, Bahrain, and Lebanon as case studies, AccessNow shows how countries adopt cybercrime laws to regulate media and state apparatus. While these laws are framed as targeting issues threatening national security, they are aimed at repressing civil rights activities, journalists, and bloggers speaking against state repression[3]. Digital repression in Nigeria is enabled by legal provisions such as the Terrorism Prevention Act and the Cybercrimes Act of 2015, global terrorism efforts such as the Financial Action Task Force Standards, and external influence from countries such as Israel and the United States. It is believed that Nigeria is trying to keep up with countries such as Russia, China, Turkey, and the United States that engage in invasive surveillance, as evidenced by increasing investments in surveillance technologies[4].

Case studies

Sudan

Sudan ranks 28–100 among free countries. By implication, a country is categorized as not free due to its experience with obstacles to access, limits on content, and violation of user rights. Internet freedom in the country is impaired by Internet disruptions due to nationwide cuts to Internet access in February. The frequent disruptions experienced in cities such as the Dafur, Khartoum, and Kordofan regions, lasting several months, have limited reliable communication and led to the repression of activists[5]. Sudan is characterized by attacks on journalists and activists, which have become incessant since the military coup of October 2021, which

[1] *Idem*
[2] Marwa Fatafta, *From Free Space to a Tool of Oppression: What Happened to the Internet Since the Arab Spring?*, "The Tahrir Institute", December 17, 2020, https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/ (09.09.2024)
[3] AccessNow, *When "Cybercrime" Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA*, September 12, 2018, https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/ (09.09.2024)
[4] Victoria Ibezim-Ohaeri, *Enabling Digital Authoritarianism in the Name of Counterterrorism: Lessons from Nigeria*, "VerfBlog", May 21, 2022, https://verfassungsblog.de/os6-nigeria/, DOI: 10.17176/20220521-182224-0
[5] Freedom House, *Sudan*, 2024, https://freedomhouse.org/country/sudan/freedom-net/2024 (09.09.2024)

deeply polarized the media. The military has overseen media-sponsoring propaganda messages, as under Omar al-Bashir's government. Since taking over through a military coup in 2021, Gen. al-Burhan, and experiencing a civil war in 2023, journalists in the country have been exposed to censorship and intimidation. They have been restricted from organizing demonstrations, arrested, and tortured to criticize the government[1]. Over 79 journalists were arrested in Sudan in 2019. This was on the heels of their engagement in anti-government protests, while some were arrested for covering protests. Government censorship increases the incidence of censorship and state surveillance[2]. Amnesty International documents extreme cases of censorship and harassment by journalists in Sudan. The National Intelligence and Security Agency (NISS) published 15 journals in 2018 and confiscated publications from print media houses. For instance, the arrest and sentencing of journalists such as Zine El Abeen Al-A'jab for allegedly disseminating false information, and the summoning of Shamel Al Nour, Ashraf Abdel Aziz, Osman Merghanie, Lina Ygoub and Maha Al Telib for holding meetings with foreign countries[3]. In addition, there are cases of newspaper confiscation and banning of television shows for interviewing militia members. The fight between the Sudan Armed Forces and paramilitary Rapid Support Forces has intensified the predicament of journalists in the country. In addition to attacking media houses, such as the General Authority for Radio and Television, they have been exposed to repeated abuse during fieldwork. Report shows that about 40 journalists have fled the country to Egypt to escape incessant abuse in the country[4].

Ethiopia

Ethiopia scores 27 over 100 on the Freedom on the Net 2024 report with obstacles to access, limits on content, and violations of user rights. As a result, the country was classified as not free in the report. Internet freedom in Ethiopia is under threat as the hostility between the federal government and rebel militias in the Amhara region escalates. This has led to the restriction of Internet services in conflict-prone areas, increasing the chances of misinformation and human rights violations. Social media platforms such as Facebook, YouTube, TikTok and Telegram were restricted while freedom of expression on the cyber space was curtailed in the Amhara region[5]. Amnesty International observes that the use of the state of emergency in Ethiopia allows the state to embark on the arbitrary arrest of dissidents, politicians, and journalists, imposing curfews, banning public assemblies, and restricting freedom of movement. For instance, journalists such as Abay Zewdu, Belay Manaye and Bekalu Alamrew were arrested and detained in 2023[6]. Media freedom in Ethiopia was threatened when the Ethiopian Media Report was politicized, leading to the promulgation of a statute that prohibits members of political parties from serving on EMA boards[7]. The data show that while Ethiopians own mobile phones, there is a lack of data connectivity. The civic space in Ethiopia is precarious, following the arrest and detaining of civil society activists, journalists, and members of the opposition. With the promulgation of emergency rule, members of the opposition, including Yohannes Buayelew, Kassa Teshager, and Christian Tadele, were detained, while staff of the Ethiopian Human Rights Council (EHRCO) were arrested in January 2023. Meanwhile, in April 2023, the Ethiopian government arrested eight journalists, including three in August, while in September, opposition leaders were beaten and arrested[8]. In these cases, due processes were not followed, whereas judicial processes were often flouted. After the outbreak of protests

[1] Reporters Without Borders, *Sudan*, 2018, https://rsf.org/en/country/sudan (01.10.2024)

[2] Reporters Without Borders, *At Least 79 Journalists Arrested in Two Months of Protests in Sudan*, 2019, https://rsf.org/en/least-79-journalists-arrested-two-months-protests-sudan (01.10.2024)

[3] Amnesty International, *Sudan: Relentless Harassment, Intimidation, and Censorship of Journalists Must End*, November 2, 2018, https://www.amnesty.org/en/latest/press-release/2018/11/sudan-relentless-harassment-intimidation-and-censorship-of-journalists-must-end/ (09.09.2024)

[4] Reporters Without Borders, *Sudan's Belligerents Are Targeting Journalists*, 2023, https://rsf.org/en/sudan-s-belligerents-are-targeting-journalists (09.09.2024)

[5] Freedom House, *Ethiopia*, 2024, https://freedomhouse.org/country/ethiopia/freedom-net/2024, (09.09.2024)

[6] Amnesty International, *Ethiopia: Authorities Must Stop Using State of Emergency Law to Silence Peaceful Dissent*, February 19, 2024, https://www.amnesty.org/en/latest/news/2024/02/ethiopia-authorities-must-stop-using-state-of-emergency-law-to-silence-peaceful-dissent/ (09.09.2024)

[7] Mulu Teka, Daniel Iberi, *Ethiopians Support Free Media Holding Government Accountable*, "Afrobarometer Dispatch" No. 801, 2024, https://www.afrobarometer.org/wp-content/uploads/2024/05/AD801-Ethiopians-support-free-media-holding-government-accountable-Afrobarometer-1may24.pdf (09.09.2024)

[8] Human Rights Watch, *Ethiopia: Events of 2023*, 2024, https://www.hrw.org/world-report/2024/country-chapters/ethiopia#0a5928 (07.09.2024)

in the Oromia region of Ethiopia, the government restricted access to social media platforms, particularly Facebook, Telegram, TikTok, and Messenger. This was initially done in 2020, when the government restricted access due to the death of a popular singer from the Oromia region[1].

Nigeria

In addition to the media clampdown, press gagging, and media censorship that pervade Nigeria's Fourth Republic, there is an increasing shrinkage of the civic space whereby activists, bloggers, and journalists have increasingly become victims of state censorship. Despite sections 22 and 39 of the country's constitution guaranteeing freedom of the press and expression as essential to good governance, cases of repression, violations, and abuse resulting in arrests, detention, threats, and torture remain unabated. The report shows that 24 journalists and media workers were killed between 1993 and 2022[2]. The use of legislation has enabled the government to crack down on media workers. Such laws include the Criminal Code Act and Cybercrimes Act of 2015. These Acts criminalize defamation and prevent cyberstalking; they have been used by the government to haunt critics and silence opposition both online and offline. Journalists such as Rotimi Jolayemi, Oluwatoyin Bolakale, Agba Jalingo, Jones Abiri, Oliver Fejiro, Luka Binniyat and Alfred Olufemi have been victims of government repression of the online media (Socio-Economic Rights and Accountability Project[3].

The Nigerian government can carry out clandestine censorship due to its unfettered access to citizen data curated from various sources, such as the Nigerian Communications Commission, responsible for licensing customers and operators, the National Identity Management Commission – in charge of the citizen database, and IMEI Policy 2021 – collating International Mobile Equipment Identity (IMEI) numbers to a Centralized Equipment Identity Register (CEIR)[4]. Governments engage in censorship through mandatory biometric data collection. In Nigeria, the government mandates that citizens register their biometric data for several services. These include: National Identity Management Commission (NIMC), Joint Admissions Matriculation Board (JAMB), West Africa Examinations Council (WAEC), National Examination Council (NECO), Independent National Electoral Commission (INEC), Federal Road Safety Commission (FRSC), Nigerian Immigration Service, TELCOS: Telecommunication operator, Banks, Nigeria Centre for Disease Control (NCDC), Foreign embassies and Integrated Payroll and Personnel information system (IPPIS) for NIN registration, exams, voter's registration, driver's license, international passport, opening of bank account, health testing, processing visas and processing payment of salaries, respectively[5]. Backed by law, these duplicate biometric collections provide the government with a complete profile of its citizens, which increases the chances of intrusion and invasion of privacy for repressive actions. The NCC is mandated to release subscribers' information and records into a central database, which can embark on the interception of communications.

The retention and interception of communication details is empowered by the Cybercrime Act 2015, which is authorized to disclose registered identity information to third parties, spyware companies, and content moderation platforms that can pull down posts suspecting spreading disinformation while the NCC can engage in network shutdown upon request from security agencies. For instance, the Nigerian military requested a network shutdown in Sokoto, Katsina, and Zamfara in September 2021 in an operation against banditry in the northwest region[6]. The rise in insecurity in Nigeria drives digital authoritarianism, as state actors are compelled to acquire digital technologies capable of identifying and tracing individuals, while occasionally engaging in surveillance and interception of private communication that undermines civil liberty and human rights[7]. While some of these sophisticated gadgets are acquired to combat terrorism and banditry, they are occasionally used to restrict online civic spaces, track activists, and restrict freedom of assembly. For instance, tactics such as Internet shutdown, social media bans, spying on opposition and activists, and biometric data collection are popular methods of engaging in state censorship. Social media bans are one of the most obvious methods for

[1] Al Jazeera, *Social Media Restricted in Ethiopia as Church Rift Turns Violent*, February 10, 2023, https://www.aljazeera.com/news/2023/2/10/social-media-restricted-in-ethiopia-after-church-rift-turns-violent (07.09.2024)
[2] SERAP, *Op. cit.,* p. 21
[3] *Ibidem*, p. 24
[4] Victoria Ibezim-Ohaeri, Joshua Olufemi, Lotanna Nwodo, Oluseyi Olufemi, Ngozi Juba-Nwosu, *Op. cit.,* p. 46
[5] *Idem*
[6] *Idem*
[7] Victoria Ibezim-Ohaeri, *Op. cit.,* p. 54

restricting citizen access and controlling the spread of information. This method has been adopted in 83 countries where popular platforms, such as Facebook, X (formerly Twitter), WhatsApp, YouTube, and Instagram, have come under attack (see Figure 9).

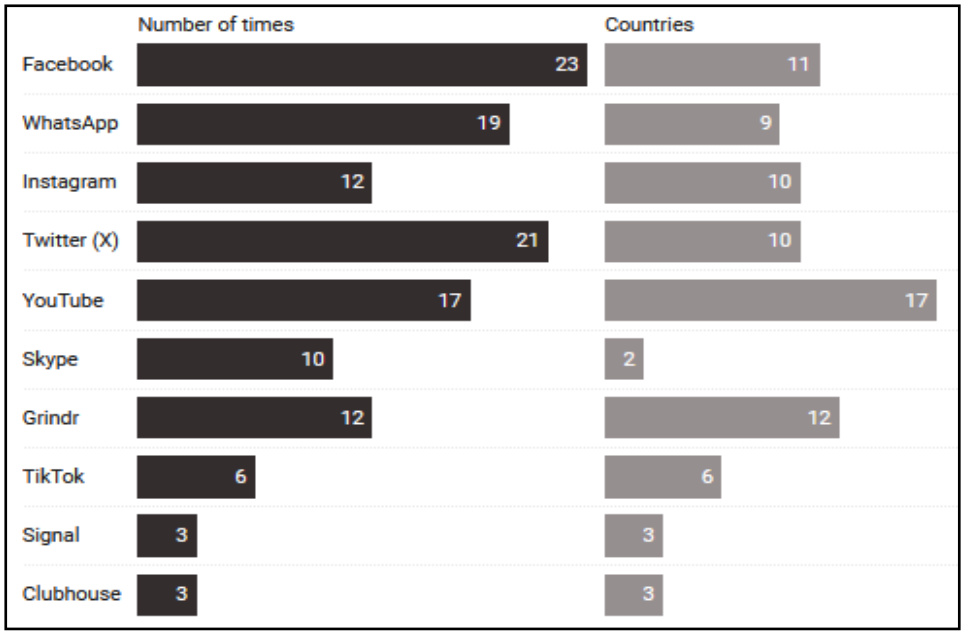

Figure 9. Incidence of Social Media Ban[1]

However, the government could not have been successful in its censorship acts without the support of private corporations such as Internet service providers, telecommunication companies, and foreign surveillance regulators such as China, Russia, and Israel[2].

Conclusions

The advent of digital technologies and their spread into Africa heralded an era of citizen empowerment and informed decision-making capabilities. With digital technologies, citizens are better equipped to take a decisive part in knowledge sharing and information production. This cascaded into politics as citizens became social critics armed with enough knowledge and information to engender social change while maintaining anonymity. The growth of digital technology and social media platforms has automatically translated into a growth in political participation, civic engagement, and enforcement of rights. With these tools, citizens are better positioned to protect their civil liberties and seek redress when such rights are truncated. However, since these tools provide citizens with avenues to hold their governments accountable, it became a double-edged sword that governments could also manipulate for their interests.

Consequently, governments, especially illiberal and authoritarian regimes, continue to seek means to adopt digital technologies to undermine citizen rights in a manner described as digital authoritarianism. While various tactics are noticeable, the use of Internet shutdowns, social media bans, Internet tax, censorship, surveillance, calls interception, and vindictive legislation are dominant. These forms of censorship not only undermine citizen rights, but also provide authoritarian governments with information to manipulate election processes, suppress opposition, and victimize dissidents.

To this end, digitalization in Africa is both a means of promoting civil rights and entrenching state censorship. Given the findings of this study, it is recommended that social media companies create a failsafe method to shield citizens from arbitrary bans, which is a clear violation of individual Internet rights. In the same manner, it is imperative that governments monitor digital companies closely to ensure that the data they collect from citizens is treated confidentially. In addition, African governments must prioritize cybersecurity through legislation and investment in digital infrastructure.

[1] International Press Institute, *Op. cit.*, p. 6
[2] Victoria Ibezim-Ohaeri, *Op. cit.*, p. 54

As a corollary, it is essential that the utmost priority is given to digital sovereignty to ensure that the digital ecosystem is protected from external interference and that citizen data is kept safe. Furthermore, civil society organizations, in conjunction with relevant stakeholders and the private sector, should invest in digital literacy to ensure that citizens are made aware of their digital rights. Finally, the role of digital rights or Internet freedom as essential to functioning and citizenship must be continuously highlighted to ensure that citizens can seek redress in the case of encroachment.

Bibliography

Books

1. Alaverdov, Emilia; Bari, Muhammad (Eds.), *Regulating Human Rights, Social Security, and Socio-Economic Structures in a Global Perspective*, IGI Global, USA, 2022
2. Roberts, Tony; Bosch, Tanja (Eds.), *Digital Citizenship in Africa: Technologies of Agency and Repression*, Zed Books, New York, 2023
3. Kperogi, Farooq, *Digital Dissidence and Social Media Censorship in Africa*, Routledge, New York, 2022
4. Servaes, Jan (Ed.), *Handbook of Communication for Development and Social Change*, Springer, Singapore, 2020

Studies and Articles

1. Akinyetun, Tope, Shola, *Democratic Backsliding in Africa: Understanding the Current Challenges*, "Kujenga Amani", Social Science Research Council, Brooklyn, 2022, https://kujenga-amani.ssrc.org/2022/09/20/democratic-backsliding-in-africa-understanding-the-current-challenges/
2. Akinyetun, Tope, Shola, *Reign of Terror: A Review of Police Brutality on Nigerian Youth by the Special Anti-Robbery Squad*, "African Security Review", Vol. 30, No. 3, 2021
3. Akinyetun, Tope, Shola, *State of Democracy in Africa: Democratic Decline or Autocracy?* "Političke Perspektive", Vol. 12, No. 2, 2022
4. Akinyetun, Tope, Shola; Ebonine, Victor, Chukwugekwu, *Digital Democracy and Democratic Decline: Unpacking the Role of Digitalization in Undermining Democracy in Africa*, "African Journal of Democracy and Election Research", Vol. 3, No. 1, 2023
5. Al Jazeera, *Social Media Restricted in Ethiopia as Church Rift Turns Violent*, February 10, 2023, https://www.aljazeera.com/news/2023/2/10/social-media-restricted-in-ethiopia-after-church-rift-turns-violent
6. CIPESA, *Sudan's Bad Laws, Internet Censorship and Repressed Civil Liberties*, 2021, https://cipesa.org/wp-content/files/briefs/Sudans_Bad_Laws_Internet_Censorship_and_Repressed_Civil_Liberties_2021.pdf
7. Fatafta, Marwa, *From Free Space to a Tool of Oppression: What Happened to the Internet Since the Arab Spring?*, The Tahrir Institute, December 17, 2020, https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/
8. Gariba, Amodani, *Enter the Dragon: The Impact of China's Digital Authoritarianism on Democracy in Africa*, The Africa Governance Papers, Vol. 1, No. 4, 2023
9. Ibezim-Ohaeri, Victoria, *Enabling Digital Authoritarianism in the Name of Counterterrorism: Lessons from Nigeria*, VerfBlog, May 21, 2022, https://verfassungsblog.de/os6-nigeria/, DOI: 10.17176/20220521-182224-0
10. Ibezim-Ohaeri, Victoria; Olufemi, Joshua; Nwodo, Lotanna; Olufemi, Oluseyi; Juba-Nwosu, Ngozi, *Security Playbook of Digital Authoritarianism in Nigeria*, Action Group on Free Civic Space, 2021, https://closingspaces.org/download/7808/?tmstv=1730893658
11. Ikorougo, Jasmine; Umeokeke, Ujunwa, *Digital Self-Sabotage: The Cost of Internet Shutdowns in Africa*, "Africa Practice", 2023, https://africapractice.com/digital-self-sabotage-the-cost-of-internet-shutdowns-in-africa/
12. Işıklı, Şevki, *Digital Citizenship: An Actual Contribution to Theory of Participatory Democracy*, "AJIT-e: Online Academic Journal of Information Technology", Vol. 6, 2015, https://doi.org/10.5824/1309-1581.2015.1.002.X

13. Kashema, Bahago; Adedeji, Adeniran; Uchenna, Efobi, *The Role of Digitalisation in Inclusive Governance: A Case Study of Sub-Saharan Africa (Occasional Paper No. 79)*, "Southern Voice", 2023
14. Laibuta, Mugambi; Hove, Kuda; Oloyede, Ridwan; Salami, Aishat, *The State of Deployment of Surveillance Technologies in Africa*, Paradigm Initiative, 2024, https://paradigmhq.org/wp-content/uploads/2024/05/The-state-of-Digital-Surveilance-1.pdf
15. Lyon, David, *Surveillance*, "Internet Policy Review", Vol. 11, No. 4, 2022, https://doi.org/10.14763/2022.4.1673
16. Manokha, Ivan, *Surveillance, Panopticism, and Self-Discipline in the Digital Age*, "Surveillance & Society", Vol. 16, No. 2, 2018
17. Manzuoli, Hennig, Cristina; Sánchez, Vargas, Ana; Bedoya, Duque, Erika, *Digital Citizenship: A Theoretical Review of the Concept and Trends*, "Turkish Online Journal of Educational Technology", Vol. 18, 2019, https://files.eric.ed.gov/fulltext/EJ1211194.pdf
18. Mlaba, Khanyi, *Africa's Internet Shutdowns: Where, Why, and How Do They Happen?*, "Global Citizen", May, 2024, https://www.globalcitizen.org/en/content/africa-internet-shutdowns-impact-human-rights/
19. Odeniyi, Solomon, *Anonymous Whistleblower, PIDOMNigeria, Arrested for Leaking Classified Documents, Others – Police*, "Punch", August 24, 2024, https://punchng.com/anonymous-whistleblower-pidomnigeria-arrested-for-leaking-classified-documents-others-police/
20. Ojakorotu, Victor, *Digitalization, Politics, and Governance in Africa*, "E-Journal of Humanities, Arts and Social Sciences", Vol. 1–2, 2023, https://doi.org/10.38159/ehass.20234141
21. Oyedemi, Toks, Dele, *Internet Access as Citizen's Right? Citizenship in the Digital Age*, "Citizenship Studies", Vol. 19, No. 3–4, 2015, pp. 450–464, https://doi.org/10.1080/13621025.2014.970441
22. Rathbone, Mark, *Panopticism, Impartial Spectator and Digital Technology*, "The Indo-Pacific Journal of Phenomenology", Vol. 22, No. 1, 2022, https://doi.org/10.1080/20797222.2022.2064720
23. Roberts, Tony, *African Governments Spend too Much on Surveillance Tech for the Wrong Reasons*, "African Liberty", November 7, 2023, https://www.africanliberty.org/2023/11/07/african-governments-spend-so-much-on-surveillance-tech-for-the-wrong-reasons/ (07.11.2023)
24. Rosson, Zach; Anthonio, Felicia; Tackett, Carolyn, *Shrinking Democracy, Growing Violence*, "Access Now", 2024, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf
25. Sesan, Gbenga, *How Africans Can Prepare for Internet Shutdowns*, "Carnegie Endowment", April 25, 2023, https://carnegieendowment.org/posts/2023/04/how-africans-can-prepare-for-internet-shutdowns?lang=en
26. Teka, Mulu; Iberi, Daniel, *Ethiopians Support Free Media Holding Government Accountable*, "Afrobarometer Dispatch", No. 801, 2024, https://www.afrobarometer.org/wp-content/uploads/2024/05/AD801-Ethiopians-support-free-media-holding-government-accountable-Afrobarometer-1may24.pdf
27. Wrobel, Claire, *Introduction: Literary and Critical Approaches to Panopticism*, "Revue d'Études Benthamiennes", Vol. 22, 2022, https://doi.org/10.4000/etudes-benthamiennes.9920

Documents

1. AccessNow, *When "Cybercrime" Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA*, 2018, https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/
2. Amnesty International, *Ethiopia: Authorities Must Stop Using State of Emergency Law to Silence Peaceful Dissent*, 2024, https://www.amnesty.org/en/latest/news/2024/02/ethiopia-authorities-must-stop-using-state-of-emergency-law-to-silence-peaceful-dissent/
3. Amnesty International, *Sudan: Relentless Harassment, Intimidation, and Censorship of Journalists Must End*, 2018, https://www.amnesty.org/en/latest/press-release/2018/11/sudan-relentless-harassment-intimidation-and-censorship-of-journalists-must-end/
4. CIPESA, *State of Internet Freedom in Africa 2024: Africa's Electoral Democracy and Technology*, 2024, https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf
5. European Investment Bank, *The Rise of Africa's Digital Economy*, European Investment Bank, Luxembourg, 2021, https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf

6. Freedom House, *Ethiopia*, 2024, https://freedomhouse.org/country/ethiopia/freedom-net/2024
7. Freedom House, *Sudan*, 2024, https://freedomhouse.org/country/sudan/freedom-net/2024
8. Freedom House, *The Mounting Damage of Flawed Elections and Armed Conflict*, Freedom House, Washington DC, 2024, https://freedomhouse.org/sites/default/files/2024-02/FIW_2024_DigitalBooklet.pdf
9. Human Rights Watch, *Ethiopia: Events of 2023*, 2024, https://www.hrw.org/world-report/2024/country-chapters/ethiopia#0a5928
10. IIAG, *Digital Freedom in Africa*, 2024, https://iiag.online/data.html?meas=DigRights&loc=AO-BF-BI-BJ-BW-CD-CF-CG-CI-CM-CV-DJ-DZ-EG-ER-ET-GA-GH-GM-GN-GQ-GW-KE-KM-LR-LS-LY-MA-MG-ML-MR-MU-MW-MZ-NA-NE-NG-RW-SC-SD-SL-SN-SO-SS-ST-SZ-TD-TG-TN-TZ-UG-ZA-ZM-ZW&view=table&subview=score&range1from=2014&range1to=2023&range2from=2019&range2to=2023&showLowest=true&showHighest=true&showEstimated=true&showTrimmed=true&showTrimmedEstimated=true&showHighlights=true&showFullContext=false&showAAT=false&sortBy=Location&sortDir=des
11. International Press Institute, *Press Freedom Violations in Africa*, IPI, 2024, https://ipi.media/wp-content/uploads/2024/07/africa-factsheet-june-2024.pdf
12. International Telecommunication Union, *The ICT Development Index 2024*, ITU, Switzerland, 2024
13. Net Blocks, *Internet Disrupted in Sudan Amid Protests Against Military Junta*, June 30, 2022, https://netblocks.org/reports/internet-disrupted-in-sudan-amid-protests-against-military-junta-QAdPrkAl
14. Reporters Without Borders, *At Least 79 Journalists Arrested in Two Months of Protests in Sudan*, 2019, https://rsf.org/en/least-79-journalists-arrested-two-months-protests-sudan
15. Reporters Without Borders, *Sudan*, 2018, https://rsf.org/en/country/sudan
16. Reporters Without Borders, *Sudan's Belligerents Are Targeting Journalists*, 2023, https://rsf.org/en/sudan-s-belligerents-are-targeting-journalists
17. Socio-Economic Rights and Accountability Project (SERAP), *Crackdown on Media Freedom and Civic Space in Nigeria*, SERAP, Lagos, 2024

Websites

1. https://africapractice.com/
2. https://carnegieendowment.org/
3. https://cipesa.org/
4. https://closingspaces.org/
5. https://files.eric.ed.gov/
6. https://freedomhouse.org/
7. https://iiag.online/
8. https://ipi.media/
9. https://kujenga-amani.ssrc.org/
10. https://netblocks.org/r
11. https://paradigmhq.org/
12. https://punchng.com/
13. https://rsf.org/en/
14. https://timep.org/
15. https://verfassungsblog.de/
16. https://www.accessnow.org/
17. https://www.africanliberty.org
18. https://www.afrobarometer.org/
19. https://www.aljazeera.com/
20. https://www.amnesty.org/
21. https://www.eib.org/
22. https://www.globalcitizen.org/
23. https://www.punchng.com/

Joanna RAK (1)
Adam Mickiewicz University of Poznań, Poland
Karolina OWCZAREK (2)
Adam Mickiewicz University of Poznań, Poland

MEDICAL POPULISM AS A MEANS OF BUILDING A POLITICAL COMMUNITY DURING PANDEMIC-INDUCED CIVIL DISORDER[1]

Abstract:	*This case study, embedded in the theoretical framework of medical populism, investigates how the TVP Info news portal, a public media entity controlled by the ruling party, strategically employed medical populism to cultivate a political community and concurrently legitimize Polish governmental actions amid the COVID-19 pandemic. The research relies on a source analysis of a population of news articles about the pandemic disseminated on TVP Info. The timeframe captures the pandemic during a transition from stringent pandemic measures to a period of eased restrictions, reduced infection rates, and a perceptible shift in focus towards the unfolding war in Ukraine.* *The study aims to unpack dimensions of medical populism existing in the narratives throughout this critical period. The analysis reveals the strategic deployment of dramatization, common-sense solutions, expertise invocation, and the dichotomy of "us" versus "them". It underscores the media's actions to shape public perception and consolidate support for the government's response to the pandemic. The conclusions drawn from this analysis contribute to enriching the understanding of how medical populism was wielded as a tool for community-building and justification of government actions during a pivotal juncture in recent history of civil disorder.*
Keywords:	**Community-building efforts; civil disorder; pandemic; medical populism; political legitimacy; legitimacy claims**
Contact details of the authors:	E-mail: joanna.rak@amu.edu.pl (1) k.owczarek16@gmail.com (2)
Institutional affiliation of the authors:	**Poznań Faculty of Political Science and Journalism, Adam Mickiewicz University, Poland (1) (2)**
Institutions address:	Poland, Poznań 61-614, ul. Uniwersytetu Poznańskiego 5, Poland (1) (2)

Introduction

The 2020 coronavirus pandemic forced governments to implement restrictions to mitigate the public health emergency[2]. Some governmental political decisions, including those of the Polish government, triggered widespread anti-government protests[3]. High was distrust towards information regarding COVID-19 spread by governments[4]. Furthermore, the Polish government stirred strong emotions to combat the pandemic, such as purchasing masks that did not meet requirements or abnormally expensive respirators from unknown medical

[1] Funding: This research paper is a result of the research project *Civil Disorder in the Pandemic-Ridden European Union*. It was financially supported by the National Science Centre, Poland [grant number 2021/43/B/HS5/00290]

[2] Nils Ringe, Lucio Rennó, *Populists and the Pandemic: How Populists Around the World Responded to COVID-19*, in N. Ringe, L. Rennó (Eds), *Populists and the Pandemic: How Populists Around the World Responded to COVID-19*", Routledge, New York, 2023

[3] Geoffrey Pleyers, *The Pandemic is a Battlefield. Social Movements in the COVID-19 Lockdown*, "Journal of Civil Society", Vol. 16, No. 4, 2020, pp. 295–312; Joanna Rak, *Pandemic-Era Civil Disorder in Post-Communist EU Member States*, Routledge, New York, 2023

[4] Marta Malesza, Magdalena C. Kaczmarek, *Predictors of Anxiety During the Covid-19 Pandemic in Poland*, "Personality and Individual Differences", Vol. 170, 2021, pp. 1-6

sources[1]. The incompetence in tackling the pandemic led to protests despite legal restrictions. Still, the largest wave of demonstrations in pandemic-stricken Poland was triggered by the Constitutional Tribunal's ruling on abortion termination. These protests took on a strongly anti-government form. In response to these protests, the government sought to employ various communication strategies, with the assistance of the Polish police, to justify their actions[2].

The pandemic was a challenge and an opportunity for the government to call for national unity and legitimise their actions. In the face of crises, citizens expect security and protection, which makes them more willing to accept social control measures larger than usual[3]. In times of public health crisis, medical populism played a significant role in efforts to claim legitimacy to the right to rule[4]. These claims are the subject of the following study, aiming to explain how, through medical populism, the government attempted to rebuild its legitimacy and build a community of Poles to whom these legitimacy demands were directed. The study contributes empirically to studies on legitimacy by enriching our understanding of the mechanism of generating authoritarian legitimacy in times of crisis.

The remainder of the article consists of four parts. The first presents a literature review on medical populism and its significance in community building. The second introduces methodological assumptions. The third discusses research findings embedded in the theoretical framework derived from the first part. The article concludes with a discussion of the role of legitimacy claims in community-building communication practices.

Literature review and theoretical framework

The category of claims to legitimacy is of growing importance in studies on stabilising political regimes. It refers to actions in which the ruling subjects determine why they are entitled to rule[5]. Recent studies indicate that claims to the right to rule fundamentally shape the governance methods of the regime and its stability[6]. Therefore, rulers must convince the ruled that they use their power competencies in the most efficient way possible, ultimately ensuring the stability of the political system. However, a significant part of society must become convinced to achieve stability. Hence, it is in rulers' interest to build a community that approves and supports their actions. Johannes Gerschewski highlights the interdependencies between rulers and the ruled and the impossibility of exercising power in the long term through power abuse[7]. Therefore, rulers, through claims to legitimacy, seek to maintain the stability of the political system. However, for this stability to occur, the opposition, the ruled, and the elites within political circles must accept the rulers' actions[8]. Thus, it is in the latter's hands to present policies in a way that convinces these groups of the justifiability of their actions. Organising a community that forms these groups is essential for stabilising political regimes.

Developing Gerschewski's theory, Christian van Soest and Julia Grauvogel[9] point out that the more pronounced the legitimisation process, the higher the probability of creating collective identification. This can

---

[1] https://wyborcza.pl/7,75398,25965040,respiratory-od-handlarza-bronia-z-czarnej-listy-onz-znamy-szczegoly.html. (3.11.2023)

[2] Joanna Rak, *Delegitimization Strategies as a Means of Policing Protesters Online During the Pandemic in Poland*, "Revista de Sociologia e Politica", Vol. 30, 2020; Joanna Rak, Karolina Owczarek *Freedom of Assembly at Stake: The Warsaw Police's Partisanship During Polish Protests in Times of Pandemi*c, "Studia Securitas", Vol. 16, No. 2, 2020, p. 175

[3] Geoffrey Pleyers, *The Pandemic is a Battlefield. Social Movements in the COVID-19 Lockdown,* "Journal of Civil Society", Vol. 16, No. 4, 2020, p. 295

[4] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020b, pp. 1–19

[5] Marcus Tannenberg, Michael Bernhard, Johannes Gerschewski, Anna Lührmann, Christian von Soest, *Claiming the Right to Rule: Regime Legitimation Strategies from 1900 to 2019*, "European Political Science Review", Vol 13, No 1, 2021, p. 79

[6] *Idem*

[7] Johannes Gerschewski, *The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes*, "Democratization", Vol. 20, No. 1, 2013, p. 13

[8] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020, p. 3

[9] Christian Van Soest, Julia Grauvogel, *How Do Non-Democratic Regimes Claim Legitimacy? Comparative Insights from Post-Soviet Countries*, GIGA Working Papers, No. 277, 2015, p. 6

facilitate the forming of a political community and positively impact the cohesion of ruling elites[1]. Simultaneously, van Soest and Grauvogel[2] emphasise that legitimisation actions can limit the spectrum of actors authorised to criticise a political regime and how criticism is expressed. A protest expresses opposition to a specific issue, which is vital for studying the Polish government's legitimacy claims during the pandemic-induced crisis, which was engulfed in anti-government protests for several months[3]. Moreover, well-formulated claims to legitimacy can influence society's perception of rulers fulfilling their political roles and reception of legitimacy claims[4]. Thus, through a carefully chosen strategy, the ruling can build a community that believes in their good intentions, thereby accepting their actions embedded in exercising power. At the same time, in addition to creating a community, rulers may deepen divisions, providing additional tools to legitimise their actions. Crises allow authoritarian leaders to gain greater legitimacy and convey the message about scenarios they create[5].

Rulers who seek legitimisation justify their appropriateness to rule and represent the ruled. They also present the expected scope of power competencies the ruled relinquish[6]. Thereby, rulers attempt to build a political community understood as a group bound by a shared commitment to public concerns, where individuals, while pursuing their interests, also recognize and uphold the conditions that sustain their collective welfare. This community is not unified by a single goal but rather by understanding the principles and boundaries of their collective identity, shaped by a narrative that legitimizes individual aspirations and communal responsibilities. Researchers use the republic category, defined as "the public concern or consideration of cives"[7], which recognises conditions and principles that bind societies together. Thus, a political community should not have a common goal but recognise the conditions defining their respublica[8]. A political community can be built through a specific narrative in which individuals still have their interests and strive to achieve them. At the same time, they want to care for public concerns, binding them together. One such public concern during the pandemic was public health, which required special protection measures. Most governments worldwide limited fundamental rights and increased power competencies[9]. These actions must have been adequately justified to avoid social opposition and generate subordination. Nevertheless, despite the populist narrative, the classical populist approach proved insufficient[10]. One reason for this could be the exogeneity of the COVID-19-induced crisis, making it initially challenging to identify a political enemy and, consequently, leading to a typically populist narrative of divisions in which someone was responsible for the crisis[11]. Therefore, rulers could seek scapegoats not necessarily accountable for causing the crisis but for its continuation or exacerbation.

---

[1] Sally N. Cummings, Ole Nørgaard, *Conceptualizing State Capacity: Comparing Kazakhstan and Kyrgyzstan*, "Political Studies", Vol. 52, No. 4, 2004, p. 685

[2] Christian Van Soest, Julia Grauvogel, *How Do Non-Democratic Regimes Claim Legitimacy? Comparative Insights from Post-Soviet Countries*, GIGA Working Papers No. 277, 2015, p. 6

[3] Joanna Rak, Karolina Owczarek, *Freedom of Assembly at Stake: The Warsaw Police's Partisanship During Polish Protests in Times of Pandemic*, "Studia Securitas", Vol. 16, No. 2, 2020, p. 172

[4] Christian Van Soest, Julia Grauvogel, *How Do Non-Democratic Regimes Claim Legitimacy? Comparative Insights from Post-Soviet Countries*, GIGA Working Papers No. 277, 2015, p. 6

[5] Elias Klenk, Julia Gurol, *The Role of Narratives for Gaining Domestic Political Legitimacy: China's Image Management during COVID-19*, "Journal of Chinese Political Science", Vol. 29, No. 1, 2024, p. 337

[6] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020, p. 3

[7] Bhikhu Parekh, *Review Article: The Political Philosophy of Michael Oakeshott*, "British Journal of Political Science", Vol. 9, No. 4, 1979, p. 495

[8] Chantal Mouffe, *Democratic Citizenship and the Political Community*, "Community at Loose Ends", edited by Miami Theory Collective, University Minnesota Press, Minnesota, 1991

[9] Douglas W. Allen, *Covid-19 Lockdown Cost/Benefits: A Critical Assessment of the Literature*, "International Journal of the Economics of Business", Vol. 29, No. 1, 2022, p. 3

[10] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020, pp. 4–5

[11] Nils Ringe, Lucio Rennó, *Populists and the Pandemic: How Populists Around the World Responded to COVID-19*, in N. Ringe, L. Rennó (Eds), *Populists and the Pandemic: How Populists Around the World Responded to COVID-19*", Routledge, New York, 2023

Exploring narratives used during public health crises, Gideon Lasco points to medical populism during the COVID-19 pandemic, in which the source of infection and crisis is the "others." However, this must be preceded by creating divisions between "us" (the people) and the "others" (those deemed dangerous)[1]. Therefore, it is essential to focus on the significance of creating a division, preceded by building a community in such a way that it gives a sense of belonging to the "people." Such division can be created by dramatizing the crisis, portraying it in an emotional, exaggerated manner to justify introducing extraordinary solutions and argue for more substantial power competencies as actions for the "people" (community)[2]. Lasco also identifies two other possible dimensions of medical populism in the pandemic. The first includes presenting quick "common-sense" solutions such as an upcoming vaccine or simplistic arguments that pit certain aspects of life (e.g., freedom and the economy) against public health. The second draws on invoking knowledge meant to simplify and present the pandemic more spectacularly. However, scientific facts do not always support this knowledge and may sometimes border on falsehood[3].

In sum, rulers claim legitimacy to maintain and strengthen their power competencies, stabilising the political system. Based on Lasco's theory, the four dimensions of medical populism narratives are creating social divisions, providing common-sense solutions, drawing on science-derived knowledge, and dramatizing. They constitute a theoretical tool for identifying claims to legitimacy concerning the public health threat that emerged with the pandemic. The application of these dimensions uncovers attempts to build a community that, during the crisis, blames the "others," the dangerous ones, for the negative impact of the pandemic on Poles. Simultaneously, the political community involves the "people." Those who oppose it are enemies considered the "others". In this context, a political community is understood as a group unified by narratives that legitimise authority by creating social divisions, often framing crises by contrasting "the people" with perceived "others." This community is bound not by shared interests or mutual goals but by a common identity constructed in opposition to those labelled as threats. In times of crisis, such as a public health emergency, this definition emphasises a collective identity reinforced by common-sense solutions, scientific rationales, and dramatic appeals to solidarity, ultimately legitimising authority through a clear distinction between the in-group and the out-group.

Methods and data

The following study rests on the theoretical frameworks presented in the second part of the article. Researchers argue that it is crucial to separate the study of medical populism from the classical approach to populism in the context of legitimacy claims[4]. Thus, this study focuses solely on the former. Medical populism refers to using populist strategies in the context of health-related issues. It involves simplifying and emotionalising complex medical information to appeal to the public. This approach often involves framing health challenges that resonate with popular sentiments, utilising charismatic figures as medical authorities, and creating a dichotomy between a "common sense" perspective and perceived elitist or expert-driven narratives. The study aims to address a research question about how the TVP Info news portal used the dimensions of medical populism to develop a political community and simultaneously justify the actions taken by the government. It is based on source analysis of news published on the TVP Info news portal, i.e., a public media entity controlled by the ruling party. It uses content analysis to unpack the dimensions of medical populism in narratives from the detection of the first COVID-19 case in Poland on March 4, 2020, until February 24, 2022. The endpoint is marked by the day the war broke out in Ukraine. Simultaneously, it was a period when restrictions were not as stringent, there were fewer reported cases of coronavirus infection, and the media shifted their focus from the coronavirus crisis that was slowly subsiding to the immigration crisis that began.

The analysis commenced with filtering news to establish the corpus of articles and videos related to the pandemic and including significant information for studying medical populism. Therefore, the news under scrutiny included the following keywords: pandemic, COVID-19, coronavirus, lockdown, and restrictions. It

[1] Gideon Lasco, *Medical Populism and the COVID-19 Pandemic*, "Global Public Health", Vol. 15, No. 10, 2020, pp. 1417–1429

[2] *Idem*

[3] *Ibidem*, pp. 1418–1419

[4] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020, p. 4

resulted in developing a corpus of 7457 news with the keyword "pandemic," 9408 with "coronavirus," 1919 with "restrictions," 1224 with "lockdown," and 9150 with "COVID-19." The analysis includes the whole news population about the pandemic, which was determined with the above criteria. To illustrate arguments in the research findings section, we choose the most frequently occurring statements that showed dimensions of medical populism. The typology presented by Lasco[1] served as a theoretical tool. Once a database of articles containing these keywords was created, they were read and viewed if they contained video materials. They were then grouped into theory-based themes and interpreted through a theoretical lens of the four dimensions of medical populism presented by Lasco[2], followed by conclusions and insights from this comparison. This process facilitated answering the research question. To maintain clarity in the study, the following section is divided into four parts, each referring to one of the dimensions of medical populism.

Research findings

The Polish government's response to the 2020 protests, which erupted in opposition to the Constitutional Tribunal's ruling on abortion, was marked by a combination of negotiated management and escalated force law enforcement and the strategic use of populist narratives to justify its actions[3]. The protests, which saw tens of thousands of citizens take to the streets, were framed by the government and state media as a threat to public order and national unity, with the protesters often depicted as lawless and disruptive. In line with the populist rhetoric of "us versus them," the ruling party and its supporters painted the demonstrators not as legitimate dissenters but as part of a broader anti-government, "dangerous" minority. This narrative was reinforced by claims that the protests posed a public health risk, especially in the context of the ongoing COVID-19 pandemic, thus allowing the government to justify its harsh response, ranging from police crackdowns to legal threats, under the guise of protecting public health and safety. The use of populist framing to discredit the protests, coupled with appeals to national solidarity, sought to solidify the government's position while portraying those who opposed it as a destabilising force, further deepening societal divisions.

Dividing a society into "us" and "them" to develop a community?

From the beginning of the pandemic in Poland, TVP Info journalists created a typical populist narrative dividing Poles into "us" and "them." The first such articles appeared in March 2020, in which the news titles suggested that the opposition spread fake news about the actions taken by the Law and Justice government[4]. The opposition was attempting to delegitimise pandemic measures and crisis management.

Another contentious issue that simultaneously opened the possibility of dividing society was the presidential elections scheduled for May 2020. TVP Info published articles emphasising that the form of elections proposed by the ruling party was the safest and best option. Meanwhile, by opposing this form, the opposition was portrayed as endangering the lives and health of Poles[5]. The construction of a community supporting postal voting was thus implemented, simultaneously distancing this community from those who opposed the idea. The division was reinforced in the fall when Poland was strongly affected by the second wave of the pandemic. Recordings from the beginning of the pandemic showed that one of the opposition politicians suggested holding elections in the fall, claiming that the pandemic would still be ongoing by then[6]. This allowed the portrayal of opposition politicians as those who did not care about public health while depicting the rulers as right in making political decisions.

The following events used to divide society were anti-government protests, specifically the entrepreneurs' strikes. Illegally imposed restrictions on public gatherings were justified by the need to care for public health. Polish law provides a mechanism for limiting the right to assemble, but it was not implemented

[1] Gideon Lasco, *Medical Populism and the COVID-19 Pandemic*, "Global Public Health", Vol. 15, No. 10, 2020, pp. 1418–1429

[2] *Idem*

[3] Joanna Rak, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020, p. 4

[4] Tvp Info, https://www.tvp.info/47112848/koronawirus-politycy-opozycji-powtarzaja-nieprawdziwe-informacje-wieszwiecej (3.11.2023)

[5] Tvp Info, https://www.tvp.info/47437311/zbigniew-ziobro-o-wyborach-prezydenckich-wieszwiecej (3.11.2023)

[6] Tvp Info, https://www.tvp.info/50430776/koronawirus-premier-wlaczyl-filmik-z-budka-szef-po-chcial-wyborow-na-jesieni-wieszwiecej (6.11.2023)

while, according to TVP Info, protesters threatened many people[1]. Thus, a division was between those who wanted to express their opposition to the regulations imposed by the Polish government and those who adhered to them. At the same time, public gatherings supporting the government were not criticised[2]. Some articles discussing pro-government assemblies did not mention how they could affect public health, while others promoted them[3].

The most significant division and the search for danger in "others" who stood against "us," the people, began after the announcement of the controversial ruling by the Constitutional Tribunal regarding abortion. Protesters took to the streets despite the illegally enforced assembly ban. In articles on the TVP Info portal, politicians from the ruling party were quoted as presenting protesters as a "threat to people's safety" when "the lives, health, and jobs of Poles are most important"[4]. Prime Minister Mateusz Morawiecki appealed for solidarity and joint action, speaking about "our shared responsibility," "let's set aside political disputes," or "let's stand together"[5]. A narrative was thus constructed in which "we," "the people," and "Poles" must have stood together to fight the coronavirus by refraining from protests. Therefore, those who opposed the calls did not want the good of the "community." Moreover, Morawiecki underscored that "health is our common concern" and "we need the solidarity cooperation of all generations and specialists from various fields to shape pro-health attitudes, promote responsibility for oneself and fellow citizens." Journalists exposed that "we" could overcome the pandemic victoriously if "we mobilise and adhere to restrictions"[6]. Thus, everyone who followed the government's orders and adhered to restrictions built a community caring for the health and lives of Poles. Over the following weeks, articles focused on the extreme irresponsibility of protesters, suggesting a high likelihood that protests would worsen the epidemic situation in Poland. It was underlined that those participating in and supporting protests disregarded Poles holding an "anti-Polish revolution"[7]. Gatherings and participation were called illegal[8]. During the peak of infections, journalists questioned whether protests held in October 2020 could have influenced the number of infections, and the answer was affirmative. People were again encouraged to refrain from protests for the good of the "community"[9]. Examples from other countries indicated that "self-discipline has slowed down the coronavirus," including measures such as limiting interpersonal contacts and movement[10].

During the third pandemic wave, the opposition was attacked again, portrayed as pressuring the government to reopen the economy a few weeks earlier than possible. When the article was published in the same week, 34 thousand infections were recorded. The same video included scrolling banners: "The stake of our actions is the lives of Poles" and "Prime Minister: 'We need national solidarity'"[11]. Besides, Morawiecki addressed an appeal to the opposition, emphasising that they did not know how to act in solidarity with the government and asked not to worsen the situation[12]. These actions divided society: opposition politicians worsened the epidemic in Poland, whereas the Polish government did everything it could to ensure public health and safety.

---

[1] Tvp Info, https://www.tvp.info/48174224/koronawirus-zgromadzenia-publiczne-szef-mswia-mariusz-kaminski-prawo-do-wyrazania-pogladow-politycznych-jest-swiete-wieszwiecej (6.11.2023)

[2] Tvp Info, https://www.tvp.info/48324331/demonstracja-poparcia-dla-czerwcowego-terminu-wyborow-wieszwiecej. (6.11.2023)

[3] Tvp Info, https://www.tvp.info/48305160/wybory-prezydenckie-manifestacja-przed-sejmem-wieszwiecej (6.11.2023)

[4] https://www.tvp.info/50474629/koronawirus-wyprowadzil-tysiace-kobiet-na-ulice-posel-po-atakuje-prezesa-pis-tuz-po-apelu-premiera-o-jednosc-w-obliczu-pandemii-wieszwiecej (6.11.2023)

[5] Tvp Info https://www.tvp.info/50473578/pandemia-premier-morawiecki-apeluje-o-solidarnosc (6.11.2023)

[6] Tvp Info, https://www.tvp.info/50501845/koronawirus-polska-zakazenia-premier-wierze-ze-przejdziemy-pandemie-zwyciesko-ale-musimy-przestrzegac-obostrzen-wieszwiecej (6.11.2023)

[7]Tvp Info, https://www.tvp.info/50527225/przemyslaw-czarnek-o-politykach-opozycji-i-protestach-skrajna-nieodpowiedzialnosc-za-nic-maja-bezpieczenstwo-polakow-wieszwiecej (6.11.2023)

[8] Tvp Info, https://www.tvp.info/50556286/prezydent-to-ze-grupa-ludzi-wychodzi-na-ulice-to-nie-znaczy-ze-nalezy-temu-ulegac (6.11.2023)

[9] Tvp Info, https://www.tvp.info/50698503/koronawirus-poradnik-czy-strajki-mogly-wplynac-przyrost-zakazen-koronawirusem (6.11.2023)

[10] Tvp Info, https://www.tvp.info/50719733/koronawirus-japonia-dobrowolne-ograniczenia-powstrzymaly-w-japonii-sars-cov-2 (6.11.2023).

[11] Tvp Info, https://www.tvp.info/50473578/pandemia-premier-morawiecki-apeluje-o-solidarnosc (6.11.2023)

[12] Tvp Info, https://www.tvp.info/52976025/koronawirus-premier-morawiecki-atak-opozycji-na-szefa- rzadu (7.11.2023)

To sum up, TVP Info employed classic divisions into "us" and "them" and implemented a strategy in which "they" posed a threat to "our" safety. For over two years of the pandemic, an attempt was made to build a political community, including those concerned about public health and following all governmental recommendations without regard for action legality. TVP Info primarily blamed the opposition and participants of anti-government protests for jeopardising the health and lives of Poles. Moreover, a trend emerged during the analysis: someone was always to blame whenever the epidemic worsened, and another wave occurred. It was never those who managed the crisis measures.

Common-sense solutions as a remedy for the community?

In March 2020, the initial "common-sense" solutions appeared aimed at combating the pandemic. One of the first articles on the TVP Info website was entitled "An expert appeals: Let's not shake hands and keep our distance"[1]. A few days later, restrictions were introduced and presented. They limited fundamental rights and freedoms, including those related to public gatherings[2]. These measures were implemented faster and more forcefully than in other countries, justified by public health concerns. Additional restrictions were introduced the following days, including limitations on leaving the house. A sense of community was fostered by appealing to adherence to these guidelines, highlighting that if people did not comply, "we would not be able to save human lives"[3].

The subsequent common-sense solutions included the closure of forests[4]. Experts' statements were then published, pointing out that the shape of the infection curve in Poland depended on citizens and their mobilisation. Simultaneously, it was noted that the Polish government made excellent decisions at the beginning by imposing stricter restrictions than neighbouring countries[5]. The theme of compliance with regulations appeared consistently, with the same argument each time – caring for the health and lives of Poles and the economy, because a higher number of infections equalled more restrictions, leading to the closure of businesses. A sense of community was thus built among those who observed regulations. In contrast, those who opposed these solutions were portrayed as not belonging to this community, automatically acting against the community of Poles.

A significant point concerning common-sense remedies was the presidential election in 2020. The ruling party proposed postal voting, which the opposition was reluctant to agree to, citing difficulties in organising it and the need for changes in the electoral code. Nevertheless, TVP Info published articles featuring statements from crucial politicians of the ruling party, including the President of the Republic of Poland, justifying support for this decision as an element that would not endanger Poles[6]. Furthermore, articles justified postal voting abroad. Various reasons were given for why it would not be possible to vote in person, and there was also mention of the passage of a new law by the Sejm regarding the presidential elections by post in 2020[7]. On the one hand, the arguments were plausible. On the other hand, Poland has an institution of a state of emergency. It was not used despite including the implementation conditions met by the pandemic. Its imposition would have allowed for a legal postponement of the election date. This political decision of non-usage was justified in an equally populist manner by the Minister of Justice, who argued that after introducing such a state, Poland could expose itself to compensation claims from foreign companies. He argued that the primary concern was safety, not financing foreign firms[8].

---

[1] Tvp Info, https://www.tvp.info/47089709/koronawirus-epidemia-ekspert-radzi-by-sie-nie-dotykac-wieszwiecej. (7.11.2023)

[2] Tvp Info https://www.tvp.info/47114910/premier-o-zaostrzeniu-walki-z-koronawirusem-wieszwiecej. (3.11.2023)

[3] Panorama Tvp, https://panorama.tvp.pl/47257642/ograniczenia-w-przemieszczaniu?_ga=2.91409368.330922495.1699192296-2044410381.1692377639 (7.11.2023)

[4] Tvp Info, https://www.tvp.info/47266747/warszawa-koronawirus-zakaz-wstepu-do-lasu-kabackiego-jest-interpelacja-wieszwiecej (7.11.2023)

[5] Tvp Info, https://www.tvp.info/47321306/koronawirus-polska-prof-norbert-maliszewski-o-krzywej-wzrostu-zachorowan-wieszwiecej (7.11.2023)

[6]Tvp Info, https://www.tvp.info/47423334/koronawirus-prezydent-o-terminie-wyborow-wieszwiecej (7.11.2023)

[7]Tvp Info, https://www.tvp.info/47566268/koronawirus-a-wybory-glosowanie-korespondencyjne-umozliwi-polonii-powszechny-udzial-wieszwiecej (8.11.2023)

[8] Tvp Info, https://www.tvp.info/47573432/koronawirus-wybory-przeprowadzenie-wyborow-prezydenckich-jesienia-moze-narazic-znacznie-wiecej-polakow-wieszwiecej (8.11.2023)

Another wave of the coronavirus reached Poland around September 2020. It was followed by the introduction of additional restrictions and the tightening of regulations. TVP Info declared zero tolerance for disregarding the DDM (Disinfection, Distance, Masks) rule[1]. The increased argumentation for introducing additional restrictions emerged before the Constitutional Tribunal's ruling. New restrictions took effect on October 23, 2020, the day the ruling was announced, and protests began throughout Poland. The Minister of Health was quoted as convincing that they were introduced for the Polish people, and the coming weeks would be crucial for the further course of the pandemic. Hence, the DDM principle was essential and should have been respected[2]. During the following weeks, the previously mentioned articles on solidarity appeared, indicating that the limitation of fundamental rights, such as freedom of assembly, was carried out only for the good of Poles and the Polish economic situation[3]. When the fourth wave of coronavirus began, new common-sense solutions appeared. Morawiecki stated, "The more people get vaccinated, the less severe the restrictions will be, and eventually, they will disappear completely"[4]. So, the vaccine was seen as an element that could influence restrictions rather than their absence in the future. However, the period between the last two articles is a few months, so errors and a lack of control over the pandemic are visible, as well as the recurring narrative in which two main arguments appeared: the life and health of Poles and the economic situation.

In summary, TVP Info introduced common-sense remedies, ranging from presenting first-hand accounts of celebrities to reassure the public to straightforward justifications for increasingly stringent restrictions. TVP Info featured quick solutions, such as the upcoming vaccine and subsequent vaccination programme, to protect Poles from further restrictions. The arguments in the narrative primarily focused on public health and the future economic condition of the country.

Community benefiting from dramatizing?

Populist politicians in power use dramatization and exaggeration of a crisis as a justification for their actions, mainly when these actions significantly restrict civil rights and freedoms. During the pandemic outbreak in Poland, TVP Info prepared citizens for the worst: "Is it a pandemic already? Recovered individuals get infected again"; "Bolt from the blue. Merkel predicts that the coronavirus will infect up to 70 per cent of Germans"[5]. Such constructed headlines could generate the approval of Poles for restrictions that emerged just a few days later. In the early stages of the pandemic, journalists discussed the potential growth of infections and the dramatic global struggle unfolding[6]. There were also articles stating that "Europe has become the epicentre of the pandemic" emphasising that Poland was one of the first countries to introduce quarantine and movement restrictions[7]. Like previous articles, these could prepare the public for additional restrictions as proportionate and justified precautions. The Minister of Health assured that isolation worked efficiently as protection against the coronavirus and compared his role to that of a commander-in-chief during wartime[8]. Subsequent statements also focused on justifying restrictions. TVP Info intensified the message in the headline, stating, "we have a choice: closure or hundreds of dead"[9]. However, he was referring to limiting social activity to a minimum or tens of thousands of sick individuals. An essential element that could create a field for dramatization was the election crisis and the division between the ruling party, which wanted to conduct postal voting, and the

[1] Tvp Info, https://www.tvp.info/50202235/koronawirus-epidemia-duzo-zakazen-przypadkow-rzad-wprowadza-nowe-obostrzenia-sprawdz-co-sie-zmienia-nowe-przepisy-maseczki-kary-wieszwiecej (8.11.2023)

[2] Tvp Info, https://www.tvp.info/50466637/koronawirus-adam-niedzielski-w-przyszlym-tygodniu-przekonamy-sie-czy-epidemia-zaczyna-spowalniac-wieszwiecej (8.11.2023)

[3] Tvp Info https://www.tvp.info/50556286/prezydent-to-ze-grupa-ludzi-wychodzi-na-ulice-to-nie-znaczy-ze-nalezy-temu-ulegac (6.11.2023)

[4] Tvp info https://www.tvp.info/57389714/najnowszy-podcast-z-premierem-morawieckim-nt-koronawirusa-i-szczepien-kilka-tygodni-zwiekszonej-mobilizacji-i-obostrzen-to-niezbyt-wysoka-cena-za-zdrowie-i-zycie-polakow (7.11.2023)

[5] Tvp Info, https://www.tvp.info/46963045/magdalena-kawalec-segond-to-juz-pandemia-ozdrowiali-zarazaja-sie-ponownie-wieszwiecej. (9.11.2023)

[6] Tvp Info, https://www.tvp.info/47141395/minister-szumowski-koronawirus-w-polsce-wiadomo-kiedy-przypadnie-czas-najwiekszego-nasilenia-zakazen-w-polsce-wieszwiecej. (9.11.2023)

[7] Tvp Info, https://www.tvp.info/47143389/who-zakazonych-w-europie-jest-prawie-tyle-samo-co-w-chinach-wieszwiecej. (9.11.2023)

[8] Tvp Info, https://www.tvp.info/47170879/minister-zdrowia-szumowski-podal-ile-procent-spoleczenstwa-moze-sie-zarazic-koronawirusem-wieszwiecej. (9.11.2023)

[9] Tvp Info, https://www.tvp.info/47201060/koronawirus-lukasz-szumowski-oszacowal-ile-moze-byc-wkrotce-zachorowan-w-polsce-wieszwiecej. (9.11.2023)

opposition, which strove to postpone the elections. Therefore, articles like "Ziobro: Presidential elections in the fall are the opposition's madness"[1] and "Andrzej Duda: If we do not elect a president, the country will plunge into chaos"[2] emerged. The presented situation aimed to convince the audience to support the government's decisions and, through dramatization, could evoke fear and, consequently, aversion to the opposition. Moreover, journalists legitimised crisis management because, against the backdrop of their articles, the solutions proposed by the ruling party seemed rational.

During another crisis, the one caused by protests related to the Constitutional Tribunal's ruling, protesters were called "death sowers"[3]. The police spokesperson stated, "It is not the places that infect, but clusters of people"[4]. This was used to justify issuing fines to individuals who decided to participate in demonstrations and the restrictions on gatherings. In subsequent articles, there was talk of "minimising" the effects of demonstrations with possible further restrictions[5]. By depicting the situation in this way, additional restrictions could be justified. In summary, the Polish government's action pattern involved "observing" and, at the same time, dramatizing the situation so that citizens would not be surprised by subsequent government decisions when the pandemic went beyond its control. Dramatization pertained to the threat posed by the coronavirus and the opposition, justifying the implementation of postal voting and portraying protesters as a risk to the community. It aimed at legitimising actions at a specific moment.

Science for a newly built community?

TVP Info, referring to knowledge, used information on the fringes of falsehood and predicted the future when simplifying the crisis, spectacularising it, and creating divisions. At the beginning of the pandemic, journalists appealed to knowledge, discussing the possibility of 250,000 Britons dying if appropriate measures were not implemented. The article also emphasised statements from specialists that restrictions should have been maintained for 18 months or longer[6]. It used the invocation of specialists to dramatize the crisis and further legitimise additional restrictions imposed by the government.

Throughout the pandemic, the surname of Włodzimierz Gut, a virologist justifying some of the government's actions, recurred in the articles. Initial comments revolved around coronavirus testing, following criticism from an opposition representative about the government's lack of test availability for people who wanted to get tested. The virologist commented that such tests were not done "in the kitchen." Instead, it was a complex process, and testing should have only been done when necessary[7]. The issue was complex, but the virologist provided a straightforward answer to explain the inability to test more people.

The virologist named the call for more tests "health populism" and talked about testing 38 million people every five days. However, the then-presidential candidate did not mention that every resident of Poland must have been tested but that everyone should have had the right to choose and the opportunity to get tested. Subsequent statements concerned the possibility of young people not observing restrictions and potential scenarios for further imposing additional restrictions. Gut presented dark scenarios, such as closing districts or cities, and talked about the worst-case scenario in which everyone got infected, and some died[8]. Simultaneously, the government representatives denied rumours of closing cities. This same virologist also tried to predict the future. In one of the early statements, he assumed that the return of the coronavirus in the

[1] Tvp Info, https://www.tvp.info/51430500/mateusz-morawiecki-badzmy-odpowiedzialni-w-swieta-bozego-narodzenia-i-nadchodzacego-sylwestra. (9.11.2023)

[2] Tvp Info, https://www.tvp.info/47643999/prezydent-andrzej-duda-w-wywiadzie-dla-gazety-polskiej-o-koniecznosci-przeprowadzenia-wyborow-wieszwiecej (9.11.2023)

[3] Tvp Info, https://www.tvp.info/47643999/prezydent-andrzej-duda-w-wywiadzie-dla-gazety-polskiej-o-koniecznosci-przeprowadzenia-wyborow-wieszwiecej (9.11.2023)

[4] Tvp Info, https://www.tvp.info/50503035/koronawirus-policja-to-nie-miejsca-zarazaja-ale-wlasnie-skupiska-ludzi-wieszwiecej (9.11.2023)

[5] Tvp Info, https://www.tvp.info/50589316/koronawirus-protesty-premier-morawiecki-pracuje-nad-zminimalizowaniem-skutkow-protestow (8.11.2023)

[6] Tvp Info, https://www.tvp.info/47158803/koronawirus-eksperci-oszacowali-skutki-jakie-moga-spowodowac-dotychczasowe-dzialania-brytyjskiego-rzadu-wieszwiecej (10.11.2023)

[7] Tvp Info, https://www.tvp.info/47158694/prof-wlodzimierz-gut-testow-na-koronawirusa-nie-robi-sie-w-kuchni-wieszwiecej (10.11.2023)

[8] Tvp Info, https://www.tvp.info/47087536/dr-wlodzimierz-gut-mlodziez-nie-powinna-przechodzic-na-model-wloski-wieszwiecej (10.11.2023)

fall was unlikely if it was well extinguished while also recommending staying at home and isolation[1]. Before the 2020 presidential elections, TVP Info published expert opinions stating that postal voting was safe, did not increase the risk of infections, and that transmitting the coronavirus by mail posed minimal risk[2]. These opinions were used to justify holding the elections via postal voting and to justify conducting presidential elections without implementing a state of emergency.

During protests the Constitutional Tribunal's ruling, experts and virologists, mainly Gut, condemned protesters. For instance, in the article "Virologist: Protesters on the streets act extremely recklessly," journalists drew comparisons of these protests to the Italian scenario. They suggested that participants would experience social ostracism, eventually leading them to comply with the imposed regulations[3]. It aimed to show the negative consequences of protest and spark fear. Journalists relying on references to science and expert opinions strengthened divisions and discouraged protests. The appeal to expert knowledge also included an element of forecasting. Gut expressed an opinion on how many infections could occur in Poland and assessed the pandemic-fighting strategy as pre-emptive moves necessary in case of an increase[4]. The same expert, a few days and a few weeks later, commented on the effectiveness of these restrictions, their initial effects, and predictions about future infection declines[5]. This was meant to justify and simplify the understanding of restrictions. However, shortly after that, new restrictions were introduced, and when Gut was asked about them, he expressed support, justifying it by stating, "What was allowed has been abused"[6]. Thus, a trend of supporting government actions and those who unquestionably complied with bans and condemning those who did not comply was evident. Gut uncritically embraced the COVID-19-fighting strategy employed by the ruling party, but citizens were always blamed for the increase in infections.

Gut also sought answers to questions about the rise in infections when the COVID-19 vaccine was already available. He noticed that the development of the pandemic would depend on people, particularly pointing out that those who did not believe in the coronavirus were harmful. According to him, too few people were vaccinated to impact the virus spread rate[7]. Expert knowledge served to simplify an explanation of increases in infections. Returning to the supportive opinions of Gut before the fourth wave of infections, he indicated that it would be a "falka" (slight wave) (suggesting a less severe wave) rather than a "fala" (wave). Furthermore, a month earlier, he supported easing restrictions[8]. However, three months later, in an interview with another virologist, it can be read that it is "high time for a local lockdown." In this article, the virologist justified the introduction of further restrictions and predicted a bleak scenario for the future of Poland during the pandemic[9]. It is noticeable how experts' statements were adjusted to the steps taken by the Polish government at a given time. This made it easier to convince and justify the imposed restrictions to the TVP Info audience.

In summary, the appeal to science and expert knowledge structured social divisions. One individual, Gut, often played the role of a significant expert. Other experts also appeared, albeit less frequently. His opinions aligned with the strategy pursued by the government, justifying the imposed restrictions. Some of the

[1] Tvp Info, https://www.tvp.info/47411502/koronawirus-w-polsce-i-europie-prof-gut-bez-ogrodek-o-pomyslach-na-lekarstwa (10.11.2023)

[2] Tvp Info, https://www.tvp.info/47723706/koronawirus-wybory-korespondencyjne-who-niskie-ryzyko-zakazenia-ekspert-o-transmisji-wirusa-przez-listy-wieszwiecej (10.11.2023)

[3] Tvp Info, https://www.tvp.info/50480373/wirusolog-protestujacy-na-polskich-ulicach-dzialaja-niezwykle-ryzykownie-wieszwiecej (10.11.2023)

[4] Tvp Info, https://www.tvp.info/50647549/pandemia-koronawirusa-polska-wirusolog-prof-wlodzimierz-gut-troche-zmniejszylismy-nasza-aktywnosc-spoleczna-i-zaczelismy-nosic-maski (10.11.2023)

[5] Tvp Info, https://www.tvp.info/47573432/koronawirus-wybory-przeprowadzenie-wyborow-prezydenckich-jesienia-moze-narazic-znacznie-wiecej-polakow-wieszwiecej (8.11.2023)

[6] Tvp Info, https://www.tvp.info/51376142/koronawirus-prof-wlodzimierz-gut-o-narodowej-kwarantannie-utrzymanie-poluzowania-grozi-nam-po-prostu-kleska. (10.11.2023)

[7] Tvp Info, https://www.tvp.info/52775749/koronawirus-gut-wzrost-zachorowan-to-efekt-braku-odpowiedzialnosci-mlodszych-rocznikow (10.11.2023)

[8] Tvp Info, https://www.tvp.info/54648799/prof-gut-nie-przewiduje-kolejnej-duzej-fali-wzrostu-zachorowan-na-covid19. (10.11.2023)

[9] Tvp Info, https://www.tvp.info/56810744/koronawirus-w-polsce-wirusolog-najwyzszy-czas-na-lokalny-lockdown (10.11.2023)

predictions were incorrect, leading readers astray. References to external expert opinions were also used to justify postal voting and simplify the issue. They allowed journalists to shift responsibility for the increase in infections onto "others" who were not part of the community following the government's directives without regard for legality.

Discussion and conclusion

TVP Info divided society and sought to depict the government's opponents as a threat. The latter included the opposition, entrepreneurs, pandemic sceptics, and those participating in protests the Constitutional Tribunal's ruling. At the same time, while dividing society, emphasis was placed on "solidarity," "acting together," and a new dimension of patriotism. Those who fully accepted and did not question the government's actions during the pandemic could belong to this community.

While simplifying the pandemic, the division and community-building also relied on the same scheme, which adhered to the principle of "those who are not with us are against us." There was an effort to argue for public health by closing places like forests. Then, there were discussions about increased controls enforcing existing regulations without implementing a state of emergency, which would have fully empowered the government to make such decisions. Nevertheless, the most prominent example of a common-sense solution was the ruling party's idea of conducting postal voting due to concerns for public health. This argument also surfaced during attempts to suppress the anti-government protests. Any restrictions on civil rights and freedoms were justified either by the above or concerns about the future state of the economy.

Simplifications also emerged regarding the upcoming vaccine, which was seen as a remedy for all the restrictions necessary during the pandemic to protect the health and lives of the community members. However, when the vaccine arrived and the coronavirus continued to threaten Poles, a simplified narrative emerged that the more people get vaccinated, the fewer restrictions would affect the community.

Dramatizing the crisis was evident from the very beginning. It was visible in headlines designed to capture the reader's attention. However, this did not occur in a single form, as problems related to the coronavirus and politicians from the ruling party, the opposition, and participants in anti-government protests were exaggerated. Once again, a narrative emerged suggesting that those who did not adhere to restrictions belonged to the "dangerous" group. Medical populism used to convey this information was vivid, intense, emotionally charged, and capable of influencing the audience. It aimed to prepare citizens for the possibility of further restrictions being imposed.

Invoking science was the final element of building community and justifying the government's right to rule. In most articles on the TVP Info website, the expert was consistently one person. Gut's opinions supported the government's actions, whether they involved tightening or loosening restrictions in Poland. He discussed the epidemiological future of Poland and often unsuccessfully tried to predict the situation. Besides, TVP Info cited external experts and their expertise on the safety of conducting elections in Poland. These opinions aligned with the government's narrative. Expert knowledge applied to dividing society into "us" and "them," simultaneously not only building a community but portraying "them" as a threat. Experts spoke on the increase in infections shortly after anti-government protests or sought responsibility for the rise in infections due to the low number of vaccinated individuals. However, it was also used as an element of dramatisation through strong, suggestive narratives used in headlines regarding new variants of the coronavirus.

All these dimensions of medical populism were used to build a political community and create a division into "us" – the community and "them" threatening the community. Anyone who unquestioningly supported the actions taken by the government and disregarded the legality of the introduced regulations could be included in the community because, at that moment, public concern (public health and the future of the economy) was the most important. The analysis reveals the strategic deployment of dramatization, common-sense solutions, expertise invocation, and the dichotomy of "us" versus "them." It underscores the media's role in shaping public perception and consolidating support for the government's pandemic response.

This article is valuable for practitioners in the fields of media studies, political communication, and public policy, as it highlights the powerful role the media can play in shaping public perception during times of crisis. By examining how TVP Info employed populist rhetoric to influence public opinion and justify government actions, the article provides key insights into how media narratives can be strategically used to divide society, consolidate support, and legitimise political decisions. For policymakers, the findings critically reflect on the potential consequences of using media to manipulate public sentiment and the ethical

implications of such practices. For media professionals, the analysis underscores the responsibility of journalists and media outlets to ensure balanced and impartial reporting, especially regarding issues that directly affect the protection of public health and civil rights. Overall, the article serves as a reminder of the importance of media literacy, critical thinking, and transparency in political communication, which are essential for maintaining democratic processes and protecting public trust.

Funding: This research paper is a result of the research project *Civil Disorder in Pandemic-ridden European Union*. It was financially supported by the National Science Centre, Poland [grant number 2021/43/B/HS5/00290].

Bibliography

Books

1. Rak, Joanna, *Pandemic-Era Civil Disorder in Post-Communist EU Member States*, Routledge, New York, 2024
2. Ringe, Nils; Rennó, Lucio (Eds.), *Populists and the Pandemic: How Populists Around the World Responded to COVID-19*, Routledge, New York, 2023

Articles

1. Allen, Douglas, W., *Covid-19 Lockdown Cost/Benefits: A Critical Assessment of the Literature*, "International Journal of the Economics of Business", Vol. 29, No. 1, 2022
2. Cummings, Sally, N., Nørgaard, Ole, *Conceptualizing State Capacity: Comparing Kazakhstan and Kyrgyzstan*, "Political Studies", Vol. 52, No. 4, 2004
3. Gerschewski, Johannes, *The Three Pillars of Stability: Legitimation, Repression, and Co-optation in Autocratic Regimes*, "Democratization", Vol. 20, No. 1, 2013
4. Klenk, Elias; Gurol, Julia, *The Role of Narratives for Gaining Domestic Political Legitimacy: China's Image Management during COVID-19*, "Journal of Chinese Political Science", Vol. 29, No. 1, 2024
5. Lasco, Gideon, *Medical Populism and the COVID-19 Pandemic*, "Global Public Health", Vol. 15, No. 10, 2020
6. Malesza, Marta; Kaczmarek, Magdalena C., *Predictors of Anxiety During the Covid-19 Pandemic in Poland*, "Personality and Individual Differences", Vol. 170, 2021
7. Mouffe, Chantal, *Democratic Citizenship and the Political Community*, "Community at Loose Ends" Miami Theory Collective, University Minnesota Press, Minnesota, 1991
8. Parekh, Bhikhu, *Review Article: The Political Philosophy of Michael Oakeshott*, "British Journal of Political Science", Vol. 9, No. 4, 1979
9. Pleyers, Geoffrey, *The Pandemic is a Battlefield. Social Movements in the COVID-19 lockdown*, "Journal of Civil Society", Vol. 16, No. 4, 2020
10. Rak, Joanna, *Delegitimization Strategies as a Means of Policing Protesters Online During the Pandemic in Poland*, "Revista de Sociologia e Politica", Vol. 30, 2020
11. Rak, Joanna; Owczarek, Karolina, *Freedom of Assembly at Stake: The Warsaw Police's Partisanship During Polish Protests in Times of Pandemic*, "Studia Securitas", Vol. 16, No. 2, 2020
12. Rak, Joanna, *The Use of Medical Populism to Claim the Right to Rule in Poland during a Public Health Emergency*, "Journal of Populism Studies", Vol. 1, No. 1, 2020
13. Tannenberg, Marcus; Bernhard, Michael; Gerschewski, Johannes; Lührmann, Anna; von Soest, Christian, *Claiming the Right to Rule: Regime Legitimation Strategies from 1900 to 2019*, "European Political Science Review", Vol. 13, No. 1, 2021
14. Van Soest, Christian; Grauvogel, Julia, *How Do Non-Democratic Regimes Claim Legitimacy? Comparative Insights from Post-Soviet Countries*, GIGA Working Papers, No. 277, 2015

Websites

1. www.panorama.tvp.pl
2. www.tvp.info
3. www.wyborcza.pl

Daiana VESMAȘ (1)
Lucian Blaga University of Sibiu, Romania
Ana MORARI (BAYRAKTAR) (2)
Lucian Blaga University of Sibiu, Romania

THE ETHICS OF E-GOVERNANCE. SAFEGUARDING DATA CONFIDENTIALITY AND HUMAN SECURITY IN PUBLIC ADMINISTRATION

Abstract:	*With the rapid digitalization of government functions, there is an emerging need for strict legal frameworks that will protect the personal data of citizens and guarantee their rights under the GDPR, adapting these provisions into the national legislative system. This legal research discusses how the need for transparency in public administration is weighed against the requirement for the confidentiality of data and how such dynamics impact human security and civil liberties.* *Considering emerging technologies such as blockchain, artificial intelligence, and automated decision-making systems, the legislative measures at present within the European Union need to be reassessed. This reassessment provides the principles of data minimization, and the legal responsibilities of both the data controller and processor in the public sector, emphasizing strongly the principles of accountability and integrity of data. The paper presented tries to provide an integral vision of data protection and human security in the digital transformation of public administration, a combination of legal and ethical considerations.*
Keywords:	**E-governance; data privacy; transparency; algorithmic fairness; digital inclusion**
Contact details of the authors:	E-mail: daiana.vesmas@ulbsibiu.ro (1) ana.morari@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Faculty of Law, Lucian Blaga University of Sibiu, Romania (1) (2)**
Institutions address:	Calea Dumbrăvii 34, Sibiu, Romania 550324 (1) (2)

Introduction

E-government is a model that manages government affairs based on the usage of local and global information networks to improve efficiency, transparency, and service delivery to citizens, thereby democratizing the processes further with the use of advanced information and communications technologies. This system of e-government information shall be used for gathering, input, searching, processing, storing, and providing information upon demand, according to user specifications, in support of the functions of government, delivery of services to individuals and organizations, and informing the public on the activity of government[1].

This rapid diffusion of e-governance has transformed public administration, allowing governments to reimagine service delivery to meet contemporary digital expectations. By digitizing essential services - such as tax filing, license applications, healthcare access, and social services distribution - governments can streamline once time-consuming and resource-intensive processes. This transformation offers citizens a more convenient,

[1] Evgenyi Romanenko, *E-Governance - A Tool for Democratization of The Public Administration System*, "International Journal of New Economics and Social Sciences", Vol. 2, No. 2, 2015, DOI: 10.5604/01.3001.0010.4772 (26.10.2024)

user-friendly way to interact with government services, reducing the need for in-person visits and long wait times, which previously presented significant barriers to accessibility[1].

Countries like Estonia with its initiative of e-Estonia, Singapore through the program Smart Nation, and India with Digital India have provided comprehensive e-governance frameworks that have set benchmarks as far as efficiency and public participation are concerned[2]. In this respect, such initiatives reflect the potential of e-governance to strengthen democratic processes through higher levels of transparency and easy access to information and services for citizens. This rapid adoption of e-governance brings in its wake malicious consequences in areas of data security, privacy, and digital inclusion. Hence, a balanced approach must be brought in to ensure that an expansion of e-governance protects individual privacy, maintains data security, and fosters equal access to digital public services throughout society[3].

This research will, therefore, be focused on the levels of ethical standards and frameworks that will be required in terms of ensuring data confidentiality and human security in digital public administration. The research will investigate the respective legal frameworks, such as the General Data Protection Regulation within the European Union, for which strict guidelines on data protection have been formulated for their efficacious application within digitalized government settings[4]. It shall further consider the ethical frameworks which may guide the responsible adoption at the core of public sector operations of digital technologies, including artificial intelligence and automated decision-making.

The evolution and digital transformation in governance

E-governance refers to the use of electronic technologies to facilitate interactions between government and citizens, businesses, and within internal government processes. Its aim is to streamline operations, enhance transparency, improve service delivery, and promote democratic engagement. E-governance simplifies administrative functions while supporting more efficient communication between various stakeholders, contributing to better decision-making and governance practices in both public and business sectors. It fosters an accessible, responsive, and more transparent government for the digital age[5].mThe evolution of e-governance began with the adoption of basic technologies to improve administrative efficiency in government operations. Initially, this involved automating internal processes to streamline bureaucratic tasks. As information and communication technology (ICT) advanced, e-governance began incorporating more interactive platforms, enabling public access to government services online and enhancing transparency[6].

By the early 2000s, the focus shifted to more citizen-centered services, fostering engagement through digital means like e-participation and e-voting, encouraging transparency, and improving government accountability. This shift marked a transition from simple automation to facilitating public participation and trust[7].

In recent years, e-governance has embraced complex, integrated solutions. Initiatives in smart cities, data analytics, and AI-driven services now cater to personalized citizen experiences and real-time service

---

[1] Carlos Rodriguez, *Digitalization in Government: Enhancing Public Service Delivery through Technology*, "Social Dynamics Review", Vol. 5, 2022, https://academicpinnacle.com/index.php/SDR/article/view/12/14 (26.10.2024)

[2] Theeraya Mayakul, Prush Sa-Nga-Ngam, Wasin Srisawat, Supaporn Kiattisin, *A Comparison of National Enterprise Architecture and e-Government Perspectives*, in *4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*, 2019, DOI: https://doi.org/10.1109/TIMES-iCON47539.2019.9024591 (26.10.2024)

[3] Oleksii Mykhalchenko, *E-Governance in The Management Decision-Making Process*, "Economic Analysis", Vol. 32, No. 1, 2022, DOI: https://doi.org/10.35774/econa2022.01.081 (26.10.2024)

[4] Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito, Nicole Monte, *The common EU approach to personal data and cybersecurity regulation*, "International Journal of Law and Information Technology", Vol. 28, No. 4, Winter, 2020, pp. 297–328, https://doi.org/10.1093/ijlit/eaaa021 (28.10.2024)

[5] Phani N. Bindu, Prem C. Sankar, Satheesh K. Kumar, *From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools*, "Government Information Quarterly", Vol. 36, No. 3, July, 2019, pp. 385-399, DOI: https://doi.org/10.1016/j.giq.2019.02.005 (28.10.2024)

[6] Åke Grönlund, Thomas A. Horan, *Introducing e-Gov: History, Definitions, and Issues*, 2004, in *Communications of the Association for Information Systems*, Vol. 15, June, 2005, DOI:10.17705/1CAIS.01539 (28.10.2024)

[7] Dmytro Khutkyy, *Citizen Engagement and Open Government Co-creation: The Cases of Brazil and the Dominican Republic*, in *Proceedings of the 24th Annual International Conference on Digital Government*, July, 2023, pp. 199-204, DOI: https://doi.org/10.1145/3598469.3598491 (28.10.2024)

delivery. Blockchain and encryption technologies address emerging concerns around data confidentiality, integrity, and security within e-governance frameworks[1].

One of the key tools of digital government nowadays is the portals of electronic public services, through which one can remotely obtain certificates, submit applications, pay fees and fines. The effectiveness of such portals is multiplied if the country has established an electronic document flow, which makes it possible to eliminate the need for paper when exchanging documents between agencies and with citizens[2].

Important for the development of digital government are cloud technologies and data storage for scaling IT infrastructure and uninterrupted operation of digital services. The states invest in information security technologies to protect personal data and secure online transactions - encryption, two-factor authentication, etc. The government develop Big Data and artificial intelligence technologies for analytics and data-based decision-making support, and distributed registries to create a trusted environment and fight corruption[3].

Legal aspects of E-governance

Transparency and security in the processing of personal data within digital systems are pursued through a series of legislative and regulatory mechanisms adopted by the international community, aiming at the protection of subjects, accountability in the management of personal data, and the avoidance of misuse or breaches.

General Data Protection Regulation (GDPR)

Ethical standards, guidelines, and frameworks of practice, such as those supported by the *General Data Protection Regulation (GDPR)* in the European Union, stand as the backbone of governance in e-governance systems. This is where it strives to ensure that personal data processing in public administrative systems will fall within the purview of commanding respect for individual privacy, transparency, and accountability. The GDPR stipulates that all personal information maintained by e-governance systems should be processed lawfully, given full consent and permission by the people, and utilized only if necessary. Key ethics linger on **data minimization**, **purpose limitation**, and ensuring data is secure[4].

The GDPR enshrines certain basic rights of data protection and privacy for individuals under Articles 12–23 of the GDPR. These include the right of access to personal data, rectification of inaccurate data, erasure- or better known as the "right to be forgotten"-restriction of processing, and data portability.[5]

For instance, in the case of contact between citizens and digital government services the GDPR encourages the adoption of privacy-preserving techniques, such as anonymization, pseudonymization, encryption, and randomization to guarantee the privacy of the personal information of a data subject undergoing any kind of processing in digital government systems[6].

Ministerial Declaration on eGovernment - the Tallinn Declaration

The Tallinn Declaration on E-Government[7] signed in 2017 by the ministers of the European Union member states, extends the general principles of their commitment to develop digital public services across Europe. Building on the success of the previous e-government initiatives, the citizen-centric, inclusive, and efficient paradigm is put at the heart of digital transformation in public administration.

---

[1] Yang Longzhi, Elisa Noe, Eliot Neil, *Privacy and Security Aspects of E-Government in Smart Cities*, "Smart Cities Cybersecurity and Privacy", 2019, pp. 89-102, DOI: https://doi.org/10.1016/B978-0-12-815032-0.00007-X (28.10.2024)

[2] Shahin Aliyev, *Digital Government: How New Technologies Improve Citizens' Lives*, in *ITCNEWS 2024*, https://ictnews.uz/23/09/2024/egovernment/ (28.10.2024)

[3] *Idem*

[4] European Commission, *Ethics and data protection*, pp. 4-6, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (28.10.2024)

[5] Damian Eke, Bernd Stahl, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, "Digital Society", Vol. 3, No. 11, 2024, DOI: https://doi.org/10.1007/s44206-024-00101-6 (28.10.2024)

[6] Razieh Nokhbeh Zaeem, Suzanne K. Barber, *The Effect of the GDPR on Privacy Policies*, "ACM Transactions on Management Information Systems (TMIS)", Vol. 12, pp. 1-20, 2020, DOI: https://doi.org/10.1145/3389685 (28.10.2024)

[7] European Comission, *Ministerial Declaration on eGovernment - the Tallinn Declaration*, 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration (28.10.2024)

The Tallinn Declaration recognized the key priorities for improvement regarding cross-border public services, user-centricity, and transparency, which ensure security in e-governance systems. Increasing access to digital services for every citizen, irrespective of the place where he/she is located, decreases bureaucratic barriers and increases access to more government services through interoperable systems across the EU. It also calls on member states to take a digital-by-default approach to the delivery of government services, allowing alternatives for those people who cannot access such services.

What is more, the declaration supports data protection and the right to privacy. It declares respect for the GDPR regarding personal data in public administration when proceeding over the e-government platforms. They also pledged to continue the development of cross-border interoperability, "enabling Union citizens and businesses to benefit from full access to digital public services across all EU member states". Therefore, this will foster not only internal mobility within the EU but also a higher degree of integration of the digital single market.

The European Declaration on Digital Rights and Principles

The EU's Declaration on Digital Rights and Principles presents six key principles. These serve as the main directors and influencers of public administration behavior across Europe as it pertains to the implementation of digital services, such as e-governance. Of these principles, the one most relevant to the context is probably "People at the Center of Digital Transformation," which mandates that public administration place citizen's needs and rights in the very center of that digital transformation. The way this principle affects and directs e-governance is not only illuminating; it also highlights the EU's overall approach to digital services[1].

The principle of Solidarity and Inclusion underscores the role of e-governance in achieving digital inclusivity, especially for vulnerable groups. This is exemplified by the Web Accessibility Directive (2016), which states that public websites and mobile applications must be accessible to people with disabilities[2]. This regulation matches the ideal of inclusive e-governance, where digital public services are accessible to all. The declaration also emphasizes the need for Sufficient Safety and Security so that public administrations can confidently engage in cross-border digital service delivery, knowing that their e-government platforms are compliant with the General Data Protection Regulation (GDPR)[3].

Compliance with this regulation is critical in e-governance because it demands that public administrations minimize the amount of personal data they collect, accounting for and protecting the data that is more likely to end up in hazard zones.

Convention for the Protection of Individuals about Automatic Processing of Personal Data

The landmark treaty established by the Council of Europe in 1981, known as the *Convention for the Protection of Individuals about Automatic Processing of Personal Data, or Convention 108*[4] modernized in steps to become Convention 108+ sets out the foundational principles to safeguard personal data and privacy. It has substantial implications for how public administrations can practice e-governance because, as a treaty, it allows signatories to hold public authorities within them accountable for how they handle personal data. As a public administration, we are bound by the principles of transparency, accountability, and proportionality that Convention 108+ embodies. Therefore, gathering and processing essential personal data within the e-governance framework must adhere to some very key tenets that were enshrined in Convention 108 and modernized in Convention 108+[5].

---

[1] European Commission, *European Digital Rights and Principles*, 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles (29.10.2024)

[2] Delia Ferri, Silvia Favalli, *Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion,* "Societies", Vol. 8, No.2, 2018, DOI:https://doi.org/10.3390/SOC8020040 (29.10.2024)

[3] European Commission, *European Digital Rights and Principles*, 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles (29.10.2024)

[4] Council of Europe, *Convention 108 +*, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (29.10.2024)

[5] Cécile de Terwangne, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, "Computer Law & Security Review, Vol. 40, April, 2021, 105497, DOI: https://doi.org/10.1016/J.CLSR.2020.105497 (30.10.2024)

While most relevant for e-governance in the EU, the focus of the Convention lies in the cross-border flow of data under Article 12[1] establishing an exchange of data between member states with uniform data protection standards that can allow public authorities to provide seamless cross-border digital services with no dent on privacy-appropriately illustrated by systems such as the European e-Justice Portal, which allows access to justice-related services by citizens across borders in the EU, while keeping up with the privacy protections of their data[2].

Ethics of E-governance

Data privacy and confidentiality

Citizens' sensitive information in e-governance is kept private and secure from unauthorized access and misuse by maintaining a robust set of Information Security Policies (ISP). A good ISP promises not just the confidentiality of data but also its integrity and availability--qualities that ensure that data remain accurate, uncorrupted, and accessible despite various types of threats that might be aimed at the government service itself. The act of e-governance, like any other online service, has to ensure not just that the right people can get in and use it (that's user authentication), but also that the wrong people can't get in[3].

In e-governance, ethical responsibilities to protect data privacy and confidentiality are countered by risks like unauthorized access, data breaches, and misuse. Public authorities must safeguard the confidentiality of sensitive information, and integrity to ensure data accuracy, and availability to prevent service disruptions.

Transparency and accountability

To quantify public trust and satisfaction, the *E-Government Transparency Index* measures citizens' perceptions of government websites, assessing factors like thoroughness, accessibility, and timeliness of information[4].

The bond connecting e-governance to transparency and accountability is vital for nurturing public trust and advancing efficient public administration. E-governance, itself an emergent form of public management, can foster this bond through the provision of electronically mediated information. For instance, indices like the *Corruption Perception Index (CPI)* and *Open Budget Index (OBI)* are used to measure transparency levels, revealing that higher transparency correlates with stronger e-governance readiness[5].

Algorithmic fairness and non-discrimination

E-governance relies on AI and automated decision-making in several critical public services, where there is a growing need to put into practice fair algorithms, unbiased and non-discriminatory. Algorithmic fairness stands for developing AI systems that treat all people fairly, without preferential treatment or disadvantage of one group against others, based on gender, ethnicity, or socio-economic background[6]. This is precisely the case with the upcoming EU AI Act, which will establish new rules on the limitation of discrimination in high-risk AI systems, including those that fall in the category of public sector AI applications. This Act will place demands for transparency, frequent auditing, and impact assessments about bias and fairness[7].

---

[1] Gregory W. Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, "International Organisations Research Journal", Vol. 17, No. 1, pp. 56–95, 2020, DOI: https://doi.org/10.17323/1996-7845-2022-01-03, (30.10.2024)

[2] Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, "European Journal of International Law", Vol. 21, No. 2, May, 2010, pp. 441-456, https://doi.org/10.1093/ejil/chq025 (30.10.2024)

[3] Shailendra Singh, *E-Governance: Information Security Issues*, in *International Conference on Computer Science and Information Technology (ICCSIT'2011)*, Pattaya Dec. 2011, pp. 120-122, https://www.researchgate.net/publication/266770761_E-Governance_Information_Security_Issues (30.10.2024)

[4] Mysore Ramaswamy, *Improving Transparency Through E-Governance*, "Information Systems", Vol. 15, No. 1, pp. 123-131, 2014, https://iacis.org/iis/2014/23_iis_2014_123-131.pdf (30.10.2024)

[5] Emad A. Abu-Shanab, *The Relationship between Transparency and E-government: An Empirical Support*, "Lecture Notes in Informatics Gesellschaft für Informatik", Bonn, 2012, pp. 85-86, https://subs.emis.de/LNI/Proceedings/Proceedings221/84.pdf (30.10.2024)

[6] Sandra Wachter, Brent Mittelstadt, Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, "Computer Law & Security Review", Vol. 41, 2021, DOI: https://doi.org/10.2139/ssrn.3547922 (30.10.2024)

[7] Matthias Wagner, Markus Borg, Per Runeson, *Navigating the Upcoming European Union AI Act*, "IEEE Software", Vol. 41, No. 1, pp. 19-24, 2024, DOI: https://doi.org/10.1109/ms.2023.3322913 (30.10.2024)

Real-world cases help in underlining that there are challenges in the implementation of fairness: the highly discussed Dutch government welfare fraud detection algorithm was alleged to discriminately point out the immigrant groups more, leading to many being wrongly accused and facing financial adversities[1]. This example underlines the need for audits of algorithms to detect biases and for public disclosure of algorithmic processes to keep transparency.

Digital inclusion and accessibility

Digital inclusion and accessibility in e-government are crucial to ensure a very ethical, fair opportunity for access to public services. It ensures that everyone, regardless of social status, age, or physical ability, will have digital service access and underpins the spirit of the European Accessibility Act 2019, which lays down a requirement that websites and mobile applications of public services must be accessible for persons with disabilities[2].

According to the United Nations E-Government Development Index, countries with more inclusive digital strategies tend to have high rankings in the satisfaction and engagement of the public.[3] Closing the digital divide necessitates that governments address challenges such as internet availability, affordability, and digital literacy, among many others. This is well evidenced in the case of the Smart Nation program in Singapore, which provides training programs for elderly citizens on methods of access and usage of digital public services[4].

Ethical e-government therefore needs policies that public authorities should put into place and technologically guarantee equal access to digital services irrespective of the citizen's status.

Case studies

Danish e-Government initiatives

In the early 2000s, Denmark's public sector began adopting digital communication. As part of the 'eDay 1' launch in 2003, public authorities were urged to email rather than use paper unless restricted due to security. Moving into 'eDay 2' in 2005, secure email was required for the transmission of sensitive data. The number of pieces of physical mail is targeted to be reduced by 40% in late 2005. Civil servants started getting pay statements via a secure 'e-boks' - amid some concerns over digital access[5].

The national eGovernment strategy, led by the Joint Cross-Government Cooperation Committee (STS), the eGovernment Strategy Committee (DSTG), and the Danish Agency for Digitization (DIGST), coordinates digital initiatives to ensure streamlined and secure public services. Public services are delivered across three government levels—central, regional, and municipal—necessitating seamless data flow and secure information sharing, particularly in healthcare[6].

The Danish e-government platform was developed through the important digital portals Borger.dk and Virk.dk, acting as a single entrance point for citizens and businesses, respectively. On the former, Borger.dk, multiple public services were made available, ranging from healthcare and social self-service applications to tax-related applications, including updates of personal records; it would be a one-stop service delivery for citizens. Likewise, Virk.dk, aimed at businesses, provides reporting, registration, and compliance tools. Creating these portals is all part of Denmark's larger interoperability strategy: it allows easy flow of data and one digital entrance at all levels of government. Joint resources, for example NemID-e-identification and the

[1] Melissa Heikkilä, *Dutch scandal serves as a warning for Europe over risks of using algorithms*, "Politico", https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/ (30.10.2024)

[2] European Accessibility Act, https://www.inclusion-europe.eu/european-accessibility-act/ (30.10.2024)

[3] UN E-government Knowledgebase, *E-Government Development Index (EGDI)*, https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index (30.10.2024)

[4] Gordon Kuo Siong Tan, *Citizens go digital: A discursive examination of digital payments in Singapore's Smart Nation project*, "Urban Studies", Vol. 59, pp. 2582 –2598, 2021, DOI: https://doi.org/10.1177/00420980211039407 (05.11.2024)

[5] Kim Viborg Andersen, Helle Zinner Henriksen, Eva Born Rasmussen, *Re-organizing government using IT: The Danish model //E-government in Europe*, Routledge, 2006, pp. 139-141

[6] Morten Meyerhoff Nielsen, Mika Yasouka, *An analysis of the Danish approach to eGovernment benefit realization*, "Internet Technologies and Society", 2014, pp. 5-7, https://www.researchgate.net/profile/Morten-Meyerhoff-Nielsen-2/publication/281774408_An_analysis_of_the_Danish_approach_to_eGovernment_benefit_realisation/links/564e050b08aeafc2aab16806/An-analysis-of-the-Danish-approach-to-eGovernment-benefit-realisation.pdf (05.11.2024)

digital postbox, are compulsory to use, which secures a coherent "single voice" experience on government services[1].

One risk of Denmark's e-government strategy is the potential for a digital divide, as some citizens may lack access to digital tools or skills required to fully engage with online services. This could lead to unequal access to essential public services, especially among older adults or low-income groups.

Estonia's Digital Government

Digitalization in Estonia's e-government is a well-organized infrastructure development focused on security, ease of access, and efficiency. At the heart of the operations is the X-Road platform, initiated in 2001, which enables secure data exchange between government databases. It is a decentralized system where agencies, enterprises, and citizens can converge online and support[2].

The Estonians ushered in an obligatory e-ID in 2002, enabling secure digital identification for various services related to health, education, and even voting from any part of the country. Legal-to-use digital signatures in Estonia further facilitate the processes and reduce administrative delays[3].

The Estonian e-Residency Programme, launched in 2014, is a means of providing access to Estonian digital services for non-residents. It is also touted as a painless method for entrepreneurs from anywhere in the world to run a business in a virtual European Union environment. Opening more opportunities in Estonia's digital ecosystem, this initiative supports an international community of digital entrepreneurs[4].

Strong data-privacy policies undergird these Estonian efforts, including the "once-only" principle that enables data sharing across agencies without requiring any submission of repeated inputs. Data integrity in areas such as health is protected by Blockchain. Regular assessment of the services through e-services makes sure that services are constantly improving. Interoperability across sectors saves over 800 years of working time for Estonians yearly, apparently due to increased efficiency[5].

Established in the early 2000s, this kind of infrastructure underpins 99% of the public services online, with 98% of citizens using e-IDs. It is stated that this system contributes to 2% of Estonia's GDP due to digital signatures only. It has also pioneered digital services in agriculture, automating the processes of remote sensing for compliance monitoring by satellite data, and Estonia's digital transformation-investing around 1.1-1.3% of the state budget on digitalization[6].

Singapore - program Smart Nation

Launched in 2014, Smart Nation represents a Singapore laced with digital technologies and data to improve lives, strengthen economic growth, and build a closer community. It focuses on applying Internet of Things devices, data analytics, artificial intelligence, and digital infrastructure across the board-urban mobility, healthcare, digital governance, and cybersecurity[7].

---

[1] Morten Meyerhoff Nielsen, *E-Governance Frameworks for Successful Citizen Use of Online Services: A Danish-Japanese Comparative Analysis*, "JeDEM - eJournal of eDemocracy and Open Government" Vol. 9, No. 2, pp. 68-109, 2017, https://doi.org/10.29379/jedem.v9i2.462 (05.11.2024)

[2] Kristjan Vassil, *Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, world development report*, 2016, pp. 3-4, https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf (05.11.2024)

[3] *Ibidem*, pp. 5-6

[4] Kaspar Korjus, Carlos Ivan Vargas Alvarez del Castillo, Taavi Kotka, *Perspectives for e-Residency strenghts, opportunities, weaknesses and threats*, "2017 Fourth International Conference on eDemocracy&eGovernment (ICEDEG)", pp. 177-181, 2017, DOI: https://doi.org/10.1109/ICEDEG.2017.7962530 (05.11.2024)

[5] Kristjan Vassil, *Op.cit.*, pp. 13-15

[6] OECD, *Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementatio*, "Digital Opportunities for Better Agricultural Policies", OECD Publishing, Paris, 2019, pp. 8-15, DOI: https://doi.org/10.1787/510a82b5-en (05.11.2024)

[7] Sang Keon Lee, Heeseo Rain Kwon, H. Cho, Jong-bok Kim, Donju Lee, *International Case Studies of Smart Cities: Singapore, Republic of Singapore*, in *Inter-American Development Bank (IDB), The Nature Conservancy (TNC)'s Nature Bonds Program*, No. IDB-DP-462, DOI: https://doi.org/10.18235/0000409 (05.11.2024)

Core among these is the NDI, which allows safe access through SingPass Mobile to everything from healthcare and education to financial services[1]. This facility, coupled with digital signatures, enables easy interactions throughout the public and private sectors and ensures secure online transactions[2]. Smart Governance assured better service delivery using data-informed policies. Applications such as OneService allow active citizenry participation in the reporting of issues within public services, providing more direct feedback to agencies on areas needing attention[3].

The Cyber Security Agency provides a multi-layer security model that assures safety for the digital infrastructure in Singapore. The environmental initiatives include but are not limited to intelligent meters, monitoring energy and water for more sustainable regulation[4].

Conclusions

E-governance is the innovative change in public administration, bringing efficiency, transparency, and availability of government services through digital means and networks. Digitizing tax filing, access to healthcare, and license applications smooth many of the most time-consuming tasks for governments while eradicating other problems such as bureaucratic delays. Innovative models at the level of countries like Denmark, Estonia, and Singapore demonstrate different ways in which digital governance can help boost engagement with the public, increase transparency, and promote accountability.

For instance, Denmark's e-government strategy has identified secure communication channels and single windows, such as *Borger.dk* -for citizens and *Virk.dk* -for businesses easy points of entry to public services. The Danish experience also points out the risk of a digital divide, whereby a significant share of citizens elderly, or people from low-income groups do not have the means or skills to participate in online services. Finding responses to these challenges of inclusiveness is an important element of the effort to ensure equity as digital governance develops.

Estonia's digital governance framework, driven by the X-Road network, with mandatory e-ID credentials and e-Residency for foreign participants, demonstrates well the key role of a singular and secure foundation in facilitating nearly all governmental services online.

This has paid dividends in Estonia in extraordinary gains of efficiency, adding about 2% to its economic output due to digital signatures alone and saving residents an immense amount of time every year. Furthermore, Estonia follows a “once-only” principle in commitment to data protection and uses blockchain for integrity; thus, it sets an example with its secure and citizen-oriented e-government.

Singapore's long-term Smart Nation vision connects the Internet of Things with data analytics and insightful artificial intelligence that further enhances urban mobility, healthcare systems, and ways of accessing digital services. It improves living standards and fosters economic development.

The core elements include the National Digital Identity or NDI, inclusive of SingPass Mobile for effortless interaction with the public or private sectors. Safeguarding this advanced framework are cybersecurity strategies crafted by the Cyber Security Agency. In addition, Singapore focuses on sustainability by intelligently metering and overseeing energy projects for the management of eco-friendly resource usage.

Without a solid legal backbone, securing citizens' information against theft or leaks and upholding moral codes remains elusive in implementing digital governance effectively. In Europe, user rights protection leans on pillars of clarity, permission, and the trimming down of data under the General Data Protection Regulation. This ensures that private details are managed with care. Agreements like the Tallinn Declaration along with Convention 108+ bring in seamless compatibility and safety across borders—binding rules

[1] Malyun Muhudin Hilowle, William Yeoh, Marthie Grobler, Graeme Pye, Frank Jiang, *Towards Improving the Adoption and Usage of National Digital Identity Systems*, in *ASE 22 Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, No. 223, pp. 1-6 2022, DOI: https://doi.org/10.1145/3551349.3561144 (05.11.2024)

[2] Singapore Ministry of Finance, *Singpass*, 2016, https://www.tech.gov.sg/files/media/media-releases/Annex_A___SingPass_Factsheet.pdf (05.11.2024)

[3] Singapore Ministry of National Development, *One Service Mobile App -- Making It Easier for You to Report Municipal Issues*, 2015, https://www.nas.gov.sg/archivesonline/data/pdfdoc/20150204002/mnd_press_release_(3).pdf (05.11.2024)

[4] Karen Teh, Vivy Suhendra, Soon Chia Lim, Abhik Roychoudhury, *Singapore's cybersecurity ecosystem*, “Communications of the ACM”, Vol. 63, No. 4, pp. 55-57, DOI: https://doi.org/10.1145/3378552 (06.11.2024)

designed to grant access to online services throughout European Union countries while keeping personal privacy intact.

The most topical issues of e-governance include ethics related to data privacy, algorithmic fairness, and inclusivity. Ethical frameworks, such as the EU AI Act, ensure that systems operating with AI algorithms are designed for transparency and auditing processes to prevent algorithmic discrimination, especially in high-risk AI applications applied by governments.

Some cases in real life, such as that of the Dutch welfare fraud algorithm, remind one of the needs for vigilant oversight in order not to allow biased outcomes or to protect vulnerable groups. Ethical e-governance doesn't forget the principle of digital inclusion, considering in this case all groups of citizens, including disabled people, in full accordance with the European Accessibility Act, not excluding digital training initiatives directed to elderly citizens undertaken in Singapore.

These international case studies, if taken as a whole, reveal that e-government, having sound ground on legislation, ethics, and security, raises administration to a great height. However, all of them carry a message for meeting the challenges in this area, the digital divide and data security to ensure that the benefits of digital change are equitably distributed among citizens. Setting standards in terms of accessibility, transparency, and security, these e-governance initiatives serve as models for contemporary public administration and provide guidelines to secure responsive, inclusive, and accountable governments in the digital era.

Bibliography

Book

1. Andersen, Kim, Viborg; Henriksen, Helle, Zinner; Rasmussen, Eva, Born, *Re-organizing government using IT: The Danish mode. E-government in Europe*, Routledge, 2006

Studies and articles

1. Abu-Shanab, Emad, A., *The Relationship between Transparency and E-government: An Empirical Support*, "Lecture Notes in Informatics Gesellschaft für Informatik", Bonn, 2012, https://subs.emis.de/LNI/Proceedings/Proceedings221/84.pdf
2. Aliyev, Shahin, *Digital Government: How New Technologies Improve Citizens' Lives*, "ITCNEWS 2024", https://ictnews.uz/23/09/2024/egovernment/
3. Bindu, Phani, N.; Sankar, Prem, C.; Satheesh, Kumar, K., *From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools*, "Government Information Quarterly", Vol. 36, No. 3, July, 2019, DOI: https://doi.org/10.1016/j.giq.2019.02.005
4. Eke, Damian; Stahl, Bernd, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, "Digital Society", Vol. 3, No.11, 2024, DOI: https://doi.org/10.1007/s44206-024-00101-6
5. Ferri, Delia; Favalli, Silvia; *Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion, "*Societies", Vol. 8, No. 2, 2018, DOI:https://doi.org/10.3390/SOC8020040
6. Grönlund, Åke; Horan, Thomas, A., *Introducing e-Gov: History, Definitions, and Issues*, 2004, "Communications of the Association for Information Systems", Vol. 15, June, 2005, DOI:10.17705/1CAIS.01539
7. Hilowle, Malyun, Muhudin; Yeoh, William; Grobler, Marthie; Pye, Graeme; Jiang, Frank; *Towards Improving the Adoption and Usage of National Digital Identity Systems*, in *ASE 22 Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, No. 223, 2022, DOI: https://doi.org/10.1145/3551349.3561144
8. Khutkyy, Dmytro, *Citizen Engagement and Open Government Co-creation: The Cases of Brazil and the Dominican Republic*, in *Proceedings of the 24th Annual International Conference on Digital Government*, July, 2023, DOI: https://doi.org/10.1145/3598469.3598491
9. Kong, Lingjie, *Data Protection and Transborder Data Flow in the European and Global Context*, "European Journal of International Law", Vol. 21, No. 2, May, 2010, https://doi.org/10.1093/ejil/chq025

10. Korjus, Kaspar; Carlos, Ivan, Vargas, Alvarez del Castillo; Kotka, Taavi, *Perspectives for e-Residency strenghts, opportunities, weaknesses and threats*, in *2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG)*, 2017, DOI: https://doi.org/10.1109/ICEDEG.2017.7962530
11. Lee, Sang Keon; Kwon, Heeseo, Rain; Cho, H.; Kim, Jong-bok; Lee, Donju, *International Case Studies of Smart Cities: Singapore, Republic of Singapore*, "Inter-American Development Bank (IDB), The Nature Conservancy (TNC)'s Nature Bonds Program" No. IDB-DP-462, DOI: https://doi.org/10.18235/0000409
12. Longzhi, Yang; Noe, Elisa; Neil, Eliot, *Privacy and Security Aspects of E-Government in Smart Cities*, "Smart Cities Cybersecurity and Privacy", 2019, DOI: https://doi.org/10.1016/B978-0-12-815032-0.00007-X
13. Mantelero, Alessandro; Vaciago, Giuseppe; Esposito, Maria, Samantha; Monte, Nicole, *The common EU approach to personal data and cybersecurity regulation*, "International Journal of Law and Information Technology, Vol. 28, No. 4, Winter, 2020, https://doi.org/10.1093/ijlit/eaaa021
14. Mayakul, Theeraya; Sa-Nga-Ngam, Prush; Srisawat, Wasin; Kiattisin, Supaporn; *A Comparison of National Enterprise Architecture and e-Government Perspectives*, in *4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*, 2019, DOI: https://doi.org/10.1109/TIMES-iCON47539.2019.9024591
15. Mykhalchenko, Oleksii, *E-Governance in The Management Decision-Making Process*, "Economic Analysis", Vol. 32, No. 1, 2022, DOI: https://doi.org/10.35774/econa2022.01.081
16. Nielsen, Morten, Meyerhoff, *E-Governance Frameworks for Successful Citizen Use of Online Services: A Danish-Japanese Comparative Analysis*, "JeDEM - eJournal of eDemocracy and Open Government", Vol. 9, No. 2, 2017, https://doi.org/10.29379/jedem.v9i2.462
17. Nielsen, Morten, Meyerhoff; Yasouka, Mika, *An analysis of the Danish approach to eGovernment benefit realization*, "Internet Technologies and Society", 2014
18. OECD, *Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation*, in *Digital Opportunities for Better Agricultural Policies*, OECD Publishing, Paris, 2019
19. Ramaswamy, Mysore, *Improving Transparency Through E-Governance*, in *Information Systems*, Vol. 15, No.1, 2014, https://iacis.org/iis/2014/23_iis_2014_123-131.pdf
20. Rodriguez, Carlos, *Digitalization in Government: Enhancing Public Service Delivery through Technology*, "Social Dynamics Review", Vol. 5, 2022, https://academicpinnacle.com/index.php/SDR/article/view/12/14
21. Romanenko, Evgeniy, *E-Governance - A Tool For Democratization of the Public Administration System*, "International Journal of New Economics And Social Sciences", Vol. 2, No. 2, 2015, DOI:10.5604/01.3001.0010.4772
22. Singh, Shailendra, *E-Governance: Information Security Issues*, "International Conference on Computer Science and Information Technology (ICCSIT'2011)", Pattaya Dec. 2011
23. Siong, Tan; Gordon, Kuo, *Citizens go digital: A discursive examination of digital payments in Singapore's Smart Nation project*, "Urban Studies", Vol. 59, 2021, DOI: https://doi.org/10.1177/00420980211039407
24. Terwangne, Cécile de, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, "Computer Law&Security Review", Vol. 40, April, 2021, 105497, DOI:https://doi.org/10.1016/J.CLSR.2020.105497
25. Teh, Karen; Suhendra, Vivy; Lim, Soon, Chia; Roychoudhury, Abhik, *Singapore's cybersecurity ecosystem*, "Communications of the ACM", Vol. 63, No. 4, DOI: https://doi.org/10.1145/3378552
26. Vassil, Kristjan, *Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, World Development Report*, 2016
27. Voss, Gregory, W., *Cross-Border Data Flows, the GDPR, and Data Governance*, "International Organisations Research Journal", Vol. 17, No. 1, 2020, DOI: https://doi.org/10.17323/1996-7845-2022-01-03
28. Wachter, Sandra; Mittelstadt, Brent; Russell, Chris, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, "Computer Law&Security Review", Vol. 41, 2021, DOI: https://doi.org/10.2139/ssrn.3547922

29. Wagner, Matthias; Borg, Markus; Runeson, Per, *Navigating the Upcoming European Union AI Act*, ”IEEE Software”, Vol. 41, No. 1, 2024, DOI: https://doi.org/10.1109/ms.2023.3322913
30. Zaeem, Razieh, Nokhbeh; Barber, Suzanne, K., *The Effect of the GDPR on Privacy Policies*, “ACM Transactions on Management Information Systems (TMIS)”, Vol. 12, 2020, DOI: https://doi.org/10.1145/3389685

Documents

1. Council of Europe, *Convention108+*, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
2. European Commission, *Ethics and data protection*, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf
3. European Commission, *European Digital Rights and Principles,* 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles
4. European Commission, *Ministerial Declaration on eGovernment - the Tallinn Declaration*, 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration
5. Inclusion Europe, *European Accessibility Act*, https://www.inclusion-europe.eu/european-accessibility-act/
6. Ministry of National Development, *One Service Mobile App -- Making It Easier for You to Report Municipal Issues*, 2015, https://www.nas.gov.sg/archivesonline/data/pdfdoc/20150204002/mnd_press_release_(3).pdf
7. Singapore Ministry of Finance, *Singpass*, 2016, https://www.tech.gov.sg/files/media/media-releases/Annex_A___SingPass_Factsheet.pdf
8. UN E-government Knowledgebase, *E-Government Development Index (EGDI)*, https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

Websites

1. https://academicpinnacle.com/
2. https://digital-strategy.ec.europa.eu/
3. https://ec.europa.eu/
4. https://iacis.org/
5. https://ictnews.uz/
6. https://publicadministration.un.org/
7. https://subs.emis.de/
8. https://www.europarl.europa.eu/
9. https://www.inclusion-europe.eu/
10. https://www.nas.gov.sg/
11. https://www.tech.gov.sg/

Ciprian NIȚU
West University of Timișoara, Romania

URBAN BOMBARDMENT AND HUMAN RIGHTS: A CRITICAL ANALYSIS OF LEGAL AND ETHICAL IMPLICATIONS OF USING WARFARE IN DENSELY POPULATED AREAS

Abstract:	*The paper examines the interaction between bombing urban areas in contemporary warfare and the competing discourses on human rights, considering the perspectives of international institutions, state actors, civil society, and victims. It explores not only the international legal frameworks governing armed conflict and human rights when urban space become the target of military operations, but also the ethical and humanitarian implications of bombardments in tightly inhabited areas, drawing attention to civilian victims, infrastructure destruction, displacement, and long-term collective trauma. It further investigates the need for a change to protect civilians more effectively in urban settings.* *Eager to contribute to ongoing legal, ethical, and policy debates on contemporary warfare and human rights, the paper leverages different methods to address the issue. It uses case study analysis, looking at recent examples of urban bombing campaigns to understand their impact on human rights. It also uses a multi-perspectival analysis of the competing discourse on the issue examining legal documents, government statements or reports by human rights organizations. Finally, the paper uses normative argumentation to advance a more cosmopolitan view on human rights on the international agenda.*
Keywords:	**Urban Warfare; aerial and artillery Bombardments; human rights; cosmopolitan law; urban security**
Contact details of the authors:	E-mail: ciprian.nitu@e-uvt.ro
Institutional affiliation of the authors:	**West University of Timișoara, Romania**
Institutions address:	Vasile Pârvan, no. 4, Timișoara, 300223, Romania

Introduction

The urban is the new geography of war. The most prominent military conflicts in the twenty-first century have unfolded in densely populated urban areas[1]. Though cities have always been crucial in warfare throughout history, recent conflicts have highlighted that urban areas have become today the central strategic battlegrounds, militarily and geopolitically[2]. The proliferation of bloody urban wars is an effect of fusion of the international, regional or domestic issues into the urban space[3]. Grozny, Aleppo, Baghdad, Mariupol, Gaza are just a few cases of sites encapsulating the problem of our world that, in a systematic and planned manner, became the targets of military violence. These cities suffered heavy aerial and artillery bombardments causing significant loss of life, destruction of built environment, and humanitarian crises.

This paper discusses the legal, ethical, and humanitarian dimensions of the warfare in densely populated areas arguing that the recent evolutions in urban geopolitics are not followed by an adequate response to protect individuals inhabiting urban space viewed as a frame for human rights substantiation. The

[1] Anthony King, *Urban Warfare in the Twenty-First Century*, Polity Press, Cambridge and Medford, 2021, pp. 4-8
[2] Sofia T. Shwayri, *Modern Warfare and the Theorization of the Middle Eastern City*, "Urban Theory Beyond the West: A World of Cities", Routledge, London and New York, 2012, p. 264
[3] Stephen Graham, *Postmortem City*, "City", Vol. 8, No. 2, 2004, p. 168

growing trend of bombing densely populated urban centers, the evolving "strategies of deliberately attacking the systems and places that support civilian urban life", the growing organized violence to "attack, destroy or annihilate urban life"[1], though not something new, are a renewed offense to human rights and dignity that has to be properly addressed and countered.

The paper answers the question how bombing campaigns in densely inhabited urban areas are addressed by international law, states and human rights advocacy, investigating the competing discourses on the issue and putting them in a new perspective that considers the city as the site of human rights realization. Hoping to contribute to ongoing legal, ethical, and policy debates on the contemporary warfare and human rights, the paper embraces a critical and normative approach arguing in support of understanding the cities as the key sites of nurturing human rights in our globalized world. Attacks on cities through aerial or artillery attacks should be seen as direct attacks on human rights.

The paper proceeds as follows. The first section discusses the theoretical background, and the methods used. After that, three recent cases of aerial and artillery bombardments are discussed to see how contemporary urban warfare raises human rights, ethical and humanitarian concerns. The subsequent section analyses the competing perspectives on civilian attacks and their protection during aerial or artillery strikes in urban areas. The analysis of these discourses is then used to assess the adequacy of international humanitarian and human rights regime in protecting individuals in urban warfare and to examine the need for a new approach.

Theory and approach

Recently, urban theory has registered a renewed interest in the city as a war space[2]. Particularly, the critical urban theory[3] looks at how urban policies and political violence intertwine resulting in well planned attack against urban sites through actions like widespread demolition of houses, strategic control of urban areas, creation of military surveillance and movement spaces, or ethnic cleansing of selected zones[4]. As a result of "a new military urbanism" the everyday urban spaces and their inhabiting civilians rendered as "threats" have become targets within a combat zone[5]. Mostly, under the slogan of "war on terror" that used to be "a kind of moral mask behind which lurk cruelty and oppression"[6], serious damage to integrity of urban space and human rights have been happening.

The extensive violence against the urban environment was referred to as "urbicide"[7]. "Urbicide" was used firstly to describe and explain the extensive devastation of Middle Eastern cities, particularly the demolition of Palestinian urban areas by the Israeli Defense Forces[8], but can be generalized to cover other cases such as destruction of cities by the Russian Federation army in the ongoing war in Ukraine. The current wars in Ukraine and Gaza have a huge impact on civilian residents, residential areas, and public spaces. The use of artillery and air strikes as a strategy of urbicide, a planned strategy to scare and kill resident population and destroy elements of urban life can be considered both urbicide and genocide, "urbicide" not being different from genocide but one of its forms[9].

---

[1] Stephen Graham, *Op. cit.*, pp. 167-171

[2] Michael Evans, *War and the City in the New Urban Century*, "*Quadrant*", January 1, 2009, https://quadrant.org.au/magazine/uncategorized/war-and-the-city-in-the-new-urban-century/(26.10.2024); Stephen Graham, *Op. cit.*, pp. 165-166, 179

[3] *Ibidem*, p. 169; Stephen Graham, *Introduction: Cities, Warfare, and States of Emergency*, "Cities, War, and Terrorism: Towards an Urban Geopolitics", Wiley-Blackwell, Malden, Oxford and Carlton, 2004, pp. 24-25; Sofia T. Shwayri, *Op. cit*., pp. 271-272

[4] Stephen Graham, *Postmortem city*, "City", Vol. 8, No. 2, 2004, pp. 170-174

[5] Stephen Graham, *Cities as Battlespace: The New Military Urbanism*, "City", Vol. 13, No. 4, 2009, pp. 383

[6] Conor Gearty, *Human Rights in an Age of Counter Terrorism*, in *War on Terror*, Manchester University Press, Manchester, 2009, p. 95

[7] Stephen Graham, *Postmortem City*, "City", Vol. 8, No. 2, 2004, pp. 177-178; Dorota Golańska, *Slow Urbicide*: *A New Materialist Account of Political Violence in Palestine*, Routledge, London, 2023; Martin Shaw, *New Wars of the City: Relationships of Urbicide and Genocide*, in *Cities, War, and Terrorism: Towards an Urban Geopolitics*, Wiley-Blackwell, Malden, Oxford, Carlton, 2004, pp. 141-153

[8] Nurhan Abujidi, *Urbicide in Palestine*: *Spaces of Oppression and Resilience*, Routledge, London, 2019; Stephen Graham, *Lessons in Urbicide*, "New Left Review", Vol. 19, 2003, pp. 63-67

[9] Martin Shaw, *Op. cit.*, p. 141

Because of perceived human rights transgressions of artillery and air bombardments and the overwhelming humanitarian consequences of urban warfare, a new strand of scholarship emerged to challenge the relevance of international humanitarian law's provisions applications and interpretations[1]. Bombing urban settlements was a strategic use of air power to determine war outcomes even since the Second World War, but despite of huge changes in strategy and means over the last decades, the condition of bombarded civilians has changed little[2]. Even though highly inconclusive militarily, bombing is chosen "to avoid combat while terrorizing non-combatants"[3] as, on the ground, the humanitarian law principle of distinction is pretty much discredited through non-enforcements by international courts[4] or non-balancing military necessity with humanitarian considerations[5]. Because the humanitarian law, when it comes to protecting civilians from bombardment, is weak and confusing, an "amalgam of morality, meta-legal processes, prophecy, terror and jurisprudential theories"[6], a new approach has been advocated, a shift that will rely more on the human rights jurisprudence and that will prove being "both more protective of victims and more politically viable than that of humanitarian law"[7].

This paper links the topic of human rights preservation with the topic of conflicts in urban zones using an approach rooted in critical urban theory that conceptualizes the city as a framework for human rights. Considering the city as a center for human rights realization, the paper looks beyond the representations of cities merely as densely populated areas, hubs of political leadership, cultural heritage spots or zones of interconnected infrastructures and services[8] to underscore the urban environment's role as a crucial space where individual rights are exercised, negotiated, and protected. Urban spaces provide the necessary infrastructure for all sorts of rights, from access to housing and learning to public health and civic participation, urban governance directly influencing quality of life and equity. As such, cities serve as practical sites for the actualization of universal human rights principles being pivotal to advancing and upholding human rights in tangible, everyday ways[9].

The paper puts forward the idea that attacks on the city in the form of aerial and artillery attacks that target urban infrastructure sustaining public life in the city, is an attack at the human rights as abilities of individuals to have a good life. Therefore, the paper will answer the question how adequate the response is this type of aggression against human rights has received thus far. To do that, it will investigate how the human rights, ethical and humanitarian issues caused by bombing campaigns in densely inhabited urban areas are addressed by international law, states and human rights advocacy. Using a multi-perspectival approach, the research focused on the most prominent international legal instruments and decisions, human rights advocacy's releases and reports, official communications by governments, and secondary literature presenting personal accounts and testimonies of individuals affected by urban warfare.

Bombarding urban areas. Human rights, ethical issues, humanitarian concerns

The artillery and aerial attacks on urban areas raise serious human rights, ethical, and humanitarian concerns. Bombardment of cities often result in high civilian casualties, destruction of residential buildings, collapse of infrastructure, and forced migration, which are a significant assault on human rights. The

[1] Mirko Sossai, *The Place of Cities in the Evolution of International Humanitarian Law*, "The Italian Yearbook of International Law Online", Vol. 31, No. 1, 2022, pp. 227-252

[2] Kenneth Hewitt, *Proving Grounds of Urbicide: Civil and Urban Perspectives on the Bombing of Capital Cities*, "ACME: An International Journal for Critical Geographies", Vol. 8, No. 2, 2009, p. 340

[3] *Idem*

[4] Jochen von Bernstorff, Enno L. Mensching, *The Dark Legacy of Nuremberg: Inhumane Air Warfare, Judicial Desuetudo and the Demise of the Principle of Distinction in International Humanitarian Law*, "Leiden Journal of International Law", Vol. 36, No. 4, 2023, pp. 1117-1118

[5] Wolff H. von Heinegg, Michael N. Schmitt (Eds.), *The Conduct of Hostilities in International Humanitarian Law*, Vol. I, Routledge, London and New York, 2023, pp. xi-xii

[6] Paul J. Goda, *The Protection of Civilians from Bombardment by Aircraft: The Ineffectiveness of the International Law of War*, "Military Law Review", Vol. 33, 1966, p. 93

[7] William Abresch, *A Human Rights Law of Internal Armed Conflict: The European Court of Human Rights in Chechnya*, "European Journal of International Law", Vol. 16, No. 4, 2005, p. 767

[8] Mirko Sossai, *Op. cit.*, pp. 227

[9] Henri Lefebvre, *Writings on Cities*, Blackwell, Oxford and Malden, 2000, pp. 147-159; David Harvey, *Rebel Cities*: *From the Right to the City to the Urban Revolution*, Verso, London and New York, 2012, pp. 3-25

indiscriminate nature of such attacks transgresses international humanitarian law that commands the safeguard of civilians during military conflicts. Targeting densely populated areas rises ethical concerns through the physical and long-term psychological harm it produces, as well as humanitarian issues caused by disruption of essential services, such as food provision, sanitation or healthcare. In the following, three recent cases of cities devastated by aerial and artillery attacks will be briefly discussed.

Aleppo has encountered massive destruction of its built environment from 2012 to 2016 during the Syrian Civil War when government forces, backed by Russian airstrikes, and opposition groups engaged in heavy combat. Aerial and artillery strikes led to widespread devastation, with entire neighborhoods reduced to ruins, particularly in rebel-held eastern Aleppo, and with water, electricity, and medical services disrupted. Civilian casualties were documented to be around twenty thousands and five hundred, with allegations of war crimes such as targeting hospitals and schools. Though all parties involved violated human rights, the indiscriminate bombings by pro-government forces contributed to higher civilian casualties[1]. Official documents by international organizations as well as academic research proved widespread human rights violations and destruction of the urban landscape. The indiscriminate military actions of the Syrian government, the use of imprecise short-range ballistic missiles and high-yield bombs in densely populated residential districts whose use had rather punitive aims than precise military objectives, are clear breaches of the international law on the rights of civilians in warfare[2].

Mariupol, a strategic port city in Ukraine, was heavily bombarded in the early months of Russia's full-scale invasion in 2022. Russian forces laid siege to the city, employing airstrikes and artillery, which destroyed critical infrastructure, including the drama theater where civilians had sought refuge. An estimated 20,000 civilians died during the siege, 200,000 citizens migrated due to loss of their homes, and the other 200,000 remaining facing a humanitarian disaster as continuing life in the city was practical impossible[3]. A report by several human rights advocacy organizations documented the devastation of Mariupol by Russian forces and called for prosecution of Russian decision makers for violations of the humanitarian law, including indiscriminate shelling and possible forced deportations of civilians[4].

Gaza City has suffered repeated cycles of violence, aerial and artillery strikes particularly, during conflicts between Israel and Palestinian armed groups. The last cycle started on October 2023 when Hamas squadrons attacked and killed civilians in the border region of Israel. As a reaction, the Israeli government started a renewed military offensive "against terror" in Gaza. Since then, Israeli airstrikes in response to Hamas rockets attacks from Gaza contributed to the continuous "brutalization"[5] of Palestinian civilians inflicting huge human casualties and infrastructure damage. As in the previous cycles of violence, civilians have paid the heavier price, with reports of residential and critical buildings being hit. Human rights organizations, media, and official authorities documented potential war crimes for all sides, both in the case of Israeli Defense Forces for disproportionate and indiscriminately hits, and Hamas for launching rockets attacks from densely populated areas. The Israeli Defense Forces's intervention in the new context might be seen in terms of continuing its urbicide policies in Gaza[6].

These are only a few, probably the most known, cases of urban warfare where aerial and artillery attacks contributed decisively to the destruction of the city and the civic life within it. For 2016, which coincides with the end of the siege of Aleppo, nearly 50 million people were believed to have been impacted by urban conflict and many of them suffered because of bombardments[7]. This represents a colossal task for

[1] Keith A. Grant, Bernd Kaussler, *The Battle of Aleppo: External Patrons and the Victimization of Civilians in Civil War*, "Small Wars and Insurgencies", Vol. 31, No. 1, 2020, pp. 1-33

[2] Andrew J. Marx, *Detecting Urban Destruction in Syria: A Landsat-Based Approach*, "Remote Sensing Applications: Society and Environment", Vol. 4, 2016, p. 30

[3] Anna Balazs, *The War on Indeterminacy: Rethinking Soviet Urban Legacy in Mariupol, 2014–2022*, "Focaal", No. 96, 2023

[4] Human Rights Watch, SITU Research, Truth Hounds, *Beneath the Rubble: Documenting Devastation and Loss in Mariupol*, https://www.hrw.org/feature/russia-ukraine-war-mariupol (11.10.2024)

[5] Stephen Graham, *Postmortem city*, "City", Vol. 8, No. 2, 2004, p. 180

[6] Stephen Graham, *Lessons in Urbicide*, "New Left Review", Vol. 19, 2003, p. 67; Sofia T. Shwayri, *Op. cit.*, pp. 264-265

[7] Vincent Bernard, *War in Cities: The Spectre of Total War*, "International Review of the Red Cross", Vol. 98, No. 901, 2016, p. 9

humanitarian organizations and should be a prime concern for international organizations that have responsibilities in this issue area.

Considering the ethical and humanitarian implications of bombardments within urban areas, as well as their impact on the urban infrastructure that upholds urban citizenship and rights[1], a question arises about how to properly see them in ethical terms. Though some justify them in terms of necessity in certain circumstances, and though there is a general agreement that bombardment carried out for the purpose of terror is unlawful[2], the view of this paper is that bombardment by artillery or from the air in urban areas is a terror act by itself and there should be a general interdiction as regards its use during urban conflicts. The recommendation is made based on the observation that, on the ground, bombardments targeting civilians to undermine their morale and loyalty was frequently used by bombing nations as strategic action, which constitutes an act of terrorism[3].

International humanitarian law and human rights law

There are two strands of international law aimed at protecting individuals that apply in different contexts and have distinct drives, the international humanitarian law and human rights law. International humanitarian law (or the "law of war") governs the actions of parties in armed conflicts with the objective of mitigating the impact of war on civilian populations. Key legal instruments of international humanitarian law are the *Hague Conventions* (1899, 1907)[4], *Geneva Conventions* (1949)[5] and their *Additional Protocols* (1977)[6]. Art. 27 of *The Hague Convention* (1907) required a certain level of care both from the attacking and defending side in case of urban bombardments and protection of non-military public buildings that are harboring civilians. Articles 48, 51, and 57 of *Additional Protocol I* deal specifically with protecting civilians from attacks, aerial and artillery included. Articles 48 and 51 establish the principle of "distinction" and prohibit indiscriminate attacks (parties must differentiate between civilians and combatants, targeting only the latter). Article 57 requires precautions to be taken to avoid civilian casualties. However, the rules against attacking civilians and civilian buildings are expressed rather in terms of simple prohibitions, without specifying the degree of care expected from the bomber, which will remain mostly a matter of subjective determination[7].

Another important instrument is *The Rome Statute of the International Criminal Court*[8] that criminalizes certain actions related to aerial bombardments like purposely directing attacks against the civilian population, strikes that cause excessive incidental civilian damage and destruction of civilian infrastructure that is not justified by military necessity, or attacks that are part of a larger plan of committed to such crimes. Besides, the customary international humanitarian law[9], which underscores rules that apply universally, like precautions (warnings, target selection and verification) or humanity in attacks is an significant additional legal basis.

Jurisprudence from international courts and tribunals is another source of humanitarian law. Court decisions from international bodies provide interpretive guidance on how aerial bombardments are framed under international law and, occasionally, judges' specific allegations of crimes against humanity. To exemplify, the International Criminal Tribunal for the Former Yugoslavia has addressed the legality of aerial bombardments during the Balkans conflict and provided specific judgments on war crimes associated with aerial bombardments in urban areas. *Case no. IT-01-42 (The Prosecutor vs. Strugar et al)* refers to charges

[1] Henri Lefebvre, *Op. cit.*, pp. 147-159; David Harvey, *Op. cit.*, pp. 3-25

[2] *Hans Blix, Area Bombardment: Rules and Reasons, in The Conduct of Hostilities in International Humanitarian Law*, Vol. I, Routledge, 2023, pp. 267-305

[3] Beau Grosscup, *Strategic Terror*: *The Politics and Ethics of Aerial Bombardment*, Zed Books, London and New York, 2006, pp. 185-186

[4] *The Hague Convention of 1899*, https://docs.pca-cpa.org/2016/01/1899-Convention-for-the-Pacific-Settlement-of-International-Disputes.pdf, (01.11.2024); *The Hague Convention of 1907*, https://ihl-databases.icrc.org/assets/treaties/195-IHL-19-EN.pdf (01.11.2024)

[5] *The Geneva Conventions of 1949*, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf, (01.11.2024)

[6] *The Additional Protocols to the Geneva Conventions (1977)*, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf (01.11.2024)

[7] William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 180

[8] *The Rome Statute of the International Criminal Court (1998)*, https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf (15.10.2024)

[9] *ICRC's Customary International Humanitarian Law Database*, https://ihl-databases.icrc.org/, (15.10.2024)

issued by the Tribunal in 2001 against four high-ranking officers of the Yugoslav People's Army, for offenses perpetrated during the occupation of the Dubrovnik region and the siege of Dubrovnik in 1991. In 2008, two of them were sentenced to 7.5 and 7 years of imprisonment, respectively, for unlawful attacks on civilians and civilian property, devastation not justified by military necessity, and destruction of religious, educational, cultural and commemorative buildings[1]. Through such decisions, the Tribunal affirmed the principle of proportionality and restrictions on attacks in urban areas and punished grave breaches of international and customary humanitarian law.

International human rights law also aims to protect individual rights, but in a broader sense. Key instruments of the human rights law such as the *Universal Declaration of Human Rights* (1948)[2], the *International Covenant on Civil and Political Rights* (1976)[3], or other regional human rights covenants like the *European Convention on Human Rights* (1953)[4] have been interpreted within the scope of military operation. The European Court of Human Rights has heard cases related to military operations, interpreting the right to life under Article 2 of the *European Convention on Human Rights* in the context of aerial bombardments affecting civilians. In its rulings, as we will see below, it has balanced international humanitarian law with human rights obligations.

Though in the context of armed conflicts both strands of international law may be applicable, international humanitarian law generally takes precedents underscoring the idea that certain human rights remain inviolable even during wartime. However, it seems there is a structural ambiguity or inconsistence within international humanitarian law. On the one hand, it affirms the non-derogability of the civilians "right to life" in wartime, on the other hand it doesn't make illegal or illegitimate aerial and artillery attacks on civilians. It only vaguely imposes some limits on these attacks, which, on the ground, may actually give the bombarding party an ample room for maneuverability. This also adds to the frequently mentioned in the academic literature of the low effectiveness of humanitarian international law in addressing use of bombardments in urban space due to "its limited substantive scope and poor record of achieving compliance in armed conflicts"[5]. As an example, though United Nations have been involved in investigating breaches of international humanitarian law in Syria since 2011 (see UN Syria Commission of Inquiry) and have been asking the Syrian government to take every possible action to prevent human rights abuses, Syria is not a party to *The Rome Statute*, the founding treaty of the International Criminal Court, and thus the Court lacks territorial jurisdiction over crimes committed within Syria.

Civil society framing of urban bombing as human rights violations

To assess the view of human rights advocacy groups on urban bombing, reports by Human Rights Watch, Amnesty International, and Doctors Without Borders on bombardments in Aleppo, Mariupol, and Gaza have been researched. These organizations have documented and condemned various strikes in the respective zones highlighting the extensive civilian harm and questioning the legality of that strikes. As regards Aleppo, Human Rights Watch reported the use of incendiary and cluster bombs in rebel-held eastern Aleppo, resulting in civilian casualties and damage to essential infrastructure[6]. Doctors Without Borders documented the impact of the bombings on medical facilities in Aleppo, including a 2016 report on the destruction of

[1] International Criminal Tribunal for the former Yugoslavia, *Case No. IT-01-42 (The Prosecutor Vs. Strugar Et Al)*, https://cld.irmct.org/assets/filings/Judgement-Strugar.pdf, (02.11.2024)

[2] *The Universal Declaration of Human Rights (1948)*, https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf, (02.11.2024)

[3] *International Covenant on Civil and Political Rights (1976)*, https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr.pdf, (02.11.2024)

[4] *The European Convention on Human Rights (1953)*, https://www.echr.coe.int/documents/d/echr/convention_ENG (02.11.2024)

[5] William Abresch, *Op. cit.*, p. 741

[6] Human Rights Watch, *Russia/Syria: War Crimes in Month of Bombing Aleppo*, https://www.hrw.org/news/2016/12/01/russia/syria-war-crimes-month-bombing-aleppo (12.11.2024)

Aleppo's hospitals by aerial bombardments[1]. These attacks were only part of a broader and systematic assault on the civilian population[2].

At Mariupol, Amnesty International's report on the Mariupol Drama Theater bombing asserted that the attack amounted to a "war crime" due to its intentional targeting of a known civilian shelter[3]. Human Rights Watch also covered the situation in Mariupol extensively, highlighting the Russian airstrikes and their effects on civilians and civilian infrastructure. A March 2022 report investigates Mariupol's siege and makes allegations of war crimes[4]. Doctors Without Borders reports as well on the ongoing humanitarian crisis in Mariupol detailing the conditions and suffering faced by civilians amid aerial bombardment[5]. In Gaza, as well, with the ongoing 2023 escalations, reports from Human Rights Watch document airstrikes that destroyed hospitals and residential buildings, including cases where there was no clear military target nearby. An April 2024 report by Human Rights Watch specifically labeled the October 31, 2023, strike on a civilian apartment building in Gaza, which killed over 100 people, as an "apparent war crime" due to the absence of a military target and failure to provide warning[6].

These sources collectively document the human rights abuses and discuss the legal implications of aerial bombardments on civilian populations in these areas, with consistent calls for international investigations, including the involvement of the International Criminal Court, to hold responsible parties for attacks that violate the laws of war and to improve protections for civilian population in such conflict zones. Generally, the human rights advocacy groups, consider that the global community and international organizations need to adopt a firmer stance on serious human rights violations in recent cases of aerial and artillery bombardments of urban areas[7]. Human rights groups often find the humanitarian law inadequate in protecting vulnerable population in armed conflicts, based on a principled and normative understanding of universality and inviolability of human rights[8]. Anyway, on the ground, humanitarian protection greatly depends on the "sound and informed" actions of the belligerent parties that, in turn, are significantly dependent on other elements like military doctrine, political will, public scrutiny or resources available[9].

The bombing states' perspective

Typically, the bombing countries describe their aerial attacks in urban areas as being legitimate, necessary and precise. In both Syria and Ukraine, Russia describes its strikes as legitimate military actions focused on "neutralizing terrorist" or "extremist" threats, protecting Russian interests, and defending the sovereignty of allied regimes such as Syria's Assad government. Russian officials claim that their actions conform to international law by focusing on military targets. In Ukraine, Russia has argued that its air strikes are aimed at degrading Ukrainian military capabilities, infrastructure, and communication networks necessary

[1] Doctors Without Borders, *Eastern Aleppo Hospitals Damaged in 23 Attacks Since July*, https://www.msf.org/syria-eastern-aleppo-hospitals-damaged-23-attacks-july (12.11.2024)

[2] Amnesty International, *Syria: Human Slaughterhouse: Mass Hangings and Extermination at Saydnaya Prison, Syria*, https://www.amnesty.org/en/documents/mde24/5415/2017/en/ (12.11.2024)

[3] Amnesty International, *Ukraine: Deadly Mariupol Theatre Strike "A Clear War Crime" by Russian Forces – New Investigation*, https://www.amnesty.org/en/latest/news/2022/06/ukraine-deadly-mariupol-theatre-strike-a-clear-war-crime-by-russian-forces-new-investigation/ (12.11.2024)

[4] Human Rights Watch, *Ukraine: New Findings on Russia's Devastation of Mariupol: War Crimes Inquiry Needed into Massive Loss of Civilian Life, Infrastructure*, https://www.hrw.org/news/2024/02/08/ukraine-new-findings-russias-devastation-mariupol (12.11.2024)

[5] Doctors Without Borders, *"We Are Calling for Respect for Human Life" in Ukraine*, https://www.msf.org/human-dignity-and-life-must-be-respected-besieged-mariupol-ukraine (12.11.2024)

[6] Human Rights Watch, *Gaza: Israeli Strike Killing 106 Civilians an Apparent War Crime: Governments Should Suspend Arms to Israel, Support ICC Probe*, https://www.hrw.org/news/2024/04/04/gaza-israeli-strike-killing-106-civilians-apparent-war-crime (12.11.2024)

[7] Anna Costa, *The Barriers and Limitations of the Modern Approach to Recognizing Genocide in Syria: A Case Study of the Sieges of Eastern Aleppo and Eastern Ghouta*, 2021, https://www.thealeppoproject.com/wp-content/uploads/2021/04/Costa_Genocide_Syria_TheAleppoProject.pdf (12.11.2024)

[8] Sean Watts, *Under Siege: International Humanitarian Law and Security Council Practice Concerning Urban Siege Operations*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479608 (25.10.2024)

[9] *Idem*

for what it frames as a "special military operation" for "denazification" and "demilitarization" of Ukraine[1]. When attacks reportedly bombarded civilian densely populated zones in Aleppo, the justification was that of attacking "terrorist strongholds"[2]. In Ukraine, similar tactics have been reported, including large-scale bombings of residential areas and civilian infrastructure such as power plants and hospitals, with Russia often attributing these to unintended collateral damage due to Ukraine's alleged use of civilians as human shields[3]. In comparison, the Israeli Defense Forces also claim legal and ethical justifications for their air strikes in Gaza. In contrast, it spends much more time and attention in presenting its attacks in terms of precision, pre-attack warning, proportionality, discrimination and humanitarian impact, than Russia usually does.

The Israeli government (through official communications from the Ministry of Foreign Affairs and other sources) frequently characterizes its air attacks in Gaza as being conducted within the framework of international law, as being reasonable actions taken in self-defense and as being morally justified in response to what it describes as "indiscriminate attacks" and "war crimes" committed by Hamas, such as rocket attacks on Israeli civilians and the October 7 attack, which Israel describes as unprecedented in brutality and scale. Israel asserts that international law permits such operations as targeting dense urban areas in defense against threats to its civilian population and national sovereignty[4].

The Israeli Defense Forces emphasizes that it takes measures to minimize harm to civilians in Gaza, highlighting its humanitarian and ethical concerns during bombardments. Israel presents its strikes as being highly targeted, focusing on "terrorist infrastructure" including weapons depots, tunnels, and operational command centers associated with Hamas. It asserts that it avoids civilian areas where possible and tries to limit unintended casualties by implementing "measured" strikes. However, Israel recognizes that some civilian casualties occur due to Hamas's alleged placement of military targets within or near civilian infrastructure, thereby complicating the task of conducting precise military operations. As well, the Israeli government warns against misinformation and encourages the public to rely on official channels to counter propaganda and "psychological warfare" efforts by Hamas[5]. Besides, Israel claims that controlled humanitarian assistance is allowed to reach civilians when possible. The measures taken aim at ensuring that humanitarian assistance get directly to civilians and is not diverted for military use by Hamas[6].

Generally, justification of aerial strikes points to shifts in contemporary urban warfare. Military strategies and technology confront now unconventional practices by the weaker side that chose cities as "places of refuge from orbital and aerial surveillance and killing"[7], trying to address diverse asymmetries of military power[8]. In the view of bombing countries, though urban warfare is not like waging war on an open battlefield by two conventional armies, with strict planning, sound strategies as well as with the help of "smart" bombs, a proper balance between strategic military objectives and protection of civilians can be kept.

However, despite the deployment of "smart" bombs, aerial strikes have led to what many commentators regard as an excessively high number of civilian casualties, particularly when contrasted with the comparatively low combatant casualties among the attacking forces[9]. Moreover, various types of

[1] TASS Russian News Agency, *Putin Declares Beginning of Military Operation in Ukraine*, February 24, 2022, https://tass.com/politics/1409329 (12.11.2024)

[2] TASS Russian News Agency, *Russian Aerospace Forces Destroy over 10 Terrorist Strongholds in Syria Killing 50 Gunmen*, February 24, 2016, https://tass.com/defense/858644 (12.11.2024)

[3] TASS Russian News Agency, *Nationalists Use Civilians as Human Shield in Kharkov Region - Russian Defense Ministry*, May 6, 2022, https://tass.com/defense/1448157 (12.11.2024).

[4] Ministry of Foreign Affairs of Israel, *Hamas-Israel Conflict 2023: Key Legal Aspects*, https://www.gov.il/BlobFolder/news/hamas-israel-conflict2023-key-legal-aspects/en/English_Documents_Hamas-Israel%20Conflict%202023%20-%20Some%20Factual%20and%20Legal%20Aspects%20-%20Israel%20Ministry%20of%20Foreign%20Affairs%20(2%20NOV%202023).pdf (25.10.2024)

[5] Israeli Government, *Swords of Iron – Updated National Talking Points*, https://govextra.gov.il/media/tudhphlu/swords-of-iron-updated-national-talking-points-26-10-23.pdf, (26.10.2023)

[6] Israeli Government, *Humanitarian Efforts*, https://gaza-aid-data.gov.il/main/ (11.11.2024)

[7] Stephen Graham, *Postmortem City*, "City", Vol. 8, No. 2, 2004, pp. 179–80

[8] Stephen Graham, *Lessons in Urbicide*, "New Left Review", Vol. 19, 2003, pp. 71–72

[9] Christine Byron, *International Humanitarian Law and Bombing Campaigns: Legitimate Military Objectives and Excessive Collateral Damage*, "Yearbook of International Humanitarian law", Vol. 13, 2010, p. 175

uncertainties make it challenging to condemn individual actions without clear evidence of intentional misconduct or severe negligence when performing aerial strikes[1].

The people and the need for a new approach

Whereas the international law and organizations, governments and civil advocacy groups are caught in a complex debate about legality, legitimacy or humanitarian effects of bombing campaigns in urban areas, the real people are those who suffer during aerial bombardments. Using the literature that collects autobiographical narratives and testimonials of affected people by warfare in urban areas, the paper looks at how they frame the aerial bombardments. Autobiographical narratives provide insights into the personal, material, and societal impacts of urban warfare while encouraging readers to empathize with the narrator. They challenge the normalized view of armed violence often presented in discussions of urban military operations, transforming these stories from mere survivor accounts into powerful political statements[2].

The testimony of individuals who have endured aerial bombardment offers a detailed and poignant portrayal of the traumatic damage inflicted by such attacks. The experiences of those affected by war and especially aerial bombardment are crucial as a way to influence and shape public opinion on this matter, to highlight the numerous detrimental effects of aerial bombardment on human beings, especially the mental health of individuals, to show how experiences of aerial and artillery bombardments instill an enduring sense of danger, and last but not least to demonstrate that "the importance of preventing threat from the air as an important human right designed to protect the safety and flourishing of individuals and communities"[3].

With this last quotation comes a suggestion for reformation of international law along a cosmopolitan path[4]. That will integrate better the perspective of people affected by harm from above, their acute psychological trauma, and the limitations imposed on their liberties and their rights in urban warfare context. The normative desirability of such a new legal framework that integrates experiences of survivors of bombings and makes the option of bombarding urban areas more and more illegal seems unquestionable. Such an approach will change the balance of international law more towards the needs and interests of people than those of governments in armed conflicts. The current international humanitarian law was successful insofar it does not offer, or seem to offer, a chance for either party to gain a strategic upper hand over the other[5]. That is, international humanitarian law is still too dependent of states' strategical interests. It is also too much dependent on other elements like reasonability and responsibility of governments. It has also low authority, specification and implementation that makes it very dissimilar when compared with the positive law[6]. Particularly problematic is the issue of how careful the attacking side has to be as "errors of judgement, mistakes, and momentary inadvertence do not constitute breaches of the international criminal law and generally do not constitute a breach of the law of targeting"[7]. Taking into consideration difficulties of maintaining the balance between humanitarian aspects and military necessity in the context of aerial warfare in modern combat operations[8], and the abundance of legal and ethical contestation of individual air attacks and broader targeting practices[9], the paper will advocate an approach that starts from a broader understanding of civilians as "citizens of urban space". As observed in the literature, legal narratives surrounding aerial

---

[1] Michael W. Lewis, *The Law of Aerial Bombardment in the 1991 Gulf War*, "American Journal of International Law", Vol. 97, No. 3, 2003, p. 508

[2] Rachel Woodward, *Narratives of Destruction and Survival: Writing and Reading About Life in Urban War Zones*, "*Theory and Event*", Vol. 10, No. 2, 2007, http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/theory_and_event/v010/10.2woodward.html (12.12.2024)

[3] Zeinab Mir, Majid Rabet, Safdar Ahmed, *Testimonies of Aerial Bombardment and Communities of Self-Expression*, "Digital War", Vol. 5, No. 1-2, 2024, pp. 94–95

[4] Ciprian Nițu, *Cosmopolitismul. Către o nouă paradigmă în teoria politică*, Adenium, Iași, 2014, pp. 224-226

[5] Hays W. Parks, *Air War and the Law of War*, in *The Conduct of Hostilities in International Humanitarian Law*, Vol. I, Routledge, 2023, p. 307

[6] Paul J. Goda, *Op. cit.*, p. 93

[7] William H. Boothby, *Op. cit.*, pp. 190–91

[8] Sean Watts, *Op. cit.*, p. 22; Wolff H. von Heinegg; Michael N. Schmitt (Eds.), *Op. cit.*, pp. xi-xii

[9] Christiane Wilke; Helyeh Doutaghi, *Legal Technologies: Conceptualizing the Legacy of the 1923 Hague Rules of Aerial Warfare*, "Leiden Journal of International Law", Vol. 37, No. 1, 2024, p. 88

bombings tend to operate under a narrow conception of civilians, thereby providing numerous excuses and justifications for targeting them in bombings[1].

This proposal goes further than the calls for changing approaches to state's tactics in urban areas, like making warnings previous of an attack more effective and specific[2], and calls for designing mechanisms to prevent conflict or helping post-conflict transitions[3]. Whereas the first approach continues to legitimize urban aerial attacks, the latter does not tell too much about protecting civilians during attacks, the accent being on prevention and post conflict strategies. The approach of this papers supports the idea of re-evaluating the relationship between human rights and humanitarian law[4]. The International Court of Justice determined that humanitarian law serves as *lex specialist* in relation to human rights law, and consequently when a case refers to human rights abuses in armed conflicts, it must be addressed by humanitarian law. But, considering the humanitarian law limitations, a changed approach has been advocated. This approach directly incorporates human rights law into the regulation of hostilities. This was the path followed, for example, by the European Court of Human Rights in its rulings on Chechnya (2005). In military conflicts, it is usually accepted that the legality of a state's artillery attacks on citizens is determined by humanitarian law, rather than human rights law, especially given the limited guidance human rights treaties offer on hostilities. The European Court of Human Rights changed the doctrine directly applying human rights law to battles involving artillery attacks and aerial bombardments, "not only without reference to humanitarian law but also in a manner that is at odds with humanitarian law"[5]. Generalizing this approach may prove practically and normatively justified in armed conflicts where humanitarian law is inadequate and frequently disregarded[6]. This approach will normatively swing the balance more towards human rights, recognizing that human rights get prominence over the security interests of states and their rights to wage war and conduct aerial attacks in an urban setting. Besides, this swing will move international law more towards a cosmopolitan law of human rights.

A cosmopolitan law of human rights applied to urban warfare will go beyond a renewed humanitarian law that will address the need to strengthen civilian protection, to maintain essential buildings and facilities, to introduce stricter accountability mechanism for states and military leaders or to "take into account the interconnected nature of a city's infrastructure when making tactical decisions"[7]. Based on understanding of cities as frameworks of human rights realization *par excellence*, it will look by all means for ways to criminalize the aerial and artillery attacks *per se* in an urban context and to recognize the multicultural and cosmopolitan dimensions of the contemporary city[8], the right of urban civilians "to live without physical or psychological threat from above" – which is something not adequately apprehended in the existing legal framework[9].

Conclusions

The paper discussed the legal, ethical, and humanitarian dimensions of the warfare in densely populated areas arguing in favor of a new approach to protect civilians more effectively in urban settings. Based on the perceived limitations of international humanitarian law documented through a multi-perspectival analysis of competing legal, official, and advocacy discourses on the "responsibility to protect" civilians during armed conflicts, the paper proposed the criminalization of the aerial and artillery bombardments within urban settings.

---

[1] Christiane Wilke, *How International Law Learned to Love the Bomb: Civilians and the Regulation of Aerial Warfare in the 1920s*, "Australian Feminist Law Journal", Vol. 44, No. 1, 2018, p. 29; Christiane Wilke; Helyeh Doutaghi, *Op. cit.*, p. 88

[2] Sharvit Baruch Pnina, Noam Neuman, *Warning Civilians Prior to Attack Under International Law: Theory and Practice*, "International Law Studies", Vol. 87, No. 16, 2011, pp. 359, 393-394

[3] Antônio Sampaio, *Before and After Urban Warfare: Conflict Prevention and Transitions in Cities*, "International Review of the Red Cross", Vol. 98, No. 901, 2016, p. 71

[4] William Abresch, *Op. cit.*

[5] *Ibidem*, p. 742

[6] *Ibidem*, p. 767

[7] Vincent Bernard, *Op. cit.*, p. 11

[8] Stephen Graham, *Postmortem City*, "City", Vol. 8, No. 2, 2004, p. 184

[9] Zeinab Mir, Majid Rabet, Safdar Ahmed, *Op. cit.*, p. 98

This proposal is normatively justified accepting the conceptualization of cities as multicultural and cosmopolitan spots, spaces that functions as frames *par excellence* for realization of human rights in the newly urbanization of politics, spaces that should become a prime concern for international organizations and institutions that have responsibilities in the issue area of protecting human rights.

Bibliography

Books

1. Abujidi, Nurhan, *Urbicide in Palestine: Spaces of Oppression and Resilience*, Routledge, London, 2019
2. Boothby, William, H., *The Law of Targeting*, Oxford University Press, Oxford, 2012
3. Golańska, Dorota, *Slow Urbicide: A New Materialist Account of Political Violence in Palestine*, Routledge, London, 2023
4. Grosscup, Beau, *Strategic Terror: The Politics and Ethics of Aerial Bombardment*, Zed Books, London&New York, 2006
5. Harvey, David, *Rebel Cities: From the Right to the City to the Urban Revolution*, Verso, London&New York, 2012
6. King, Anthony, *Urban Warfare in the Twenty-First Century*, Polity Press, Cambridge&Medford, 2021
7. Lefebvre, Henri, *Writings on Cities*, Blackwell, Oxford&Malden, 2000
8. Nițu, Ciprian, *Cosmopolitismul. Către o nouă paradigmă în teoria politică*, Adenium, Iași, 2014
9. von Heinegg, Wolff H.; Schmitt, Michael, N., (Eds.), *The Conduct of Hostilities in International Humanitarian Law*, Vol. I, Routledge, London&New York, 2023

Studies and Articles

1. Abresch, William, *A Human Rights Law of Internal Armed Conflict: The European Court of Human Rights in Chechnya*, "European Journal of International Law", Vol. 16, No. 4, 2005
2. Balazs, Anna, *The War on Indeterminacy: Rethinking Soviet Urban Legacy in Mariupol, 2014–2022*, "Focaal", No. 96, 2023
3. Baruch, Pnina, Sharvit; Neuman, Noam, *Warning Civilians Prior to Attack Under International Law: Theory and Practice*, "International Law Studies", Vol. 87, No. 16, 2011
4. Bernard, Vincent, *War in Cities: The Spectre of Total War*, "International Review of the Red Cross", Vol. 98, No. 901, 2016
5. Bernstorff, Jochen von; Enno, L., Mensching, *The Dark Legacy of Nuremberg: Inhumane Air Warfare, Judicial Desuetudo and the Demise of the Principle of Distinction in International Humanitarian Law*, "Leiden Journal of International Law", Vol. 36, No. 4, 2023
6. Blix, Hans, *Area Bombardment: Rules and Reasons*, in *The Conduct of Hostilities in International Humanitarian Law*, Vol. I, Routledge, 2023
7. Byron, Christine, *International Humanitarian Law and Bombing Campaigns: Legitimate Military Objectives and Excessive Collateral Damage*, "Yearbook of International Humanitarian Law", Vol. 13, 2010
8. Costa, Anna, *The Barriers and Limitations of the Modern Approach to Recognizing Genocide in Syria: A Case Study of the Sieges of Eastern Aleppo and Eastern Ghouta*", 2021, https://www.thealeppoproject.com/wp-content/uploads/2021/04/Costa_Genocide_Syria_TheAleppoProject.pdf
9. Gearty, Conor, *Human Rights in an Age of Counter Terrorism*, in *War on Terror*, Manchester University Press, Manchester, 2009
10. Goda, J., Paul, *The Protection of Civilians from Bombardment by Aircraft: The Ineffectiveness of the International Law of War*, "Military Law Review", Vol. 33, 1966
11. Graham, Stephen, *Cities as Battlespace: The New Military Urbanism*, "City", Vol. 13, No. 4, 2009
12. Graham, Stephen, *Introduction: Cities, Warfare, and States of Emergency*, in *Cities, War, and Terrorism: Towards an Urban Geopolitics*, Wiley-Blackwell, Malden, Oxford&Carlton, 2004
13. Graham, Stephen, *Lessons in Urbicide*, "New Left Review", Vol. 19, 2003
14. Graham, Stephen, *Postmortem City*, "City", Vol. 8, No. 2, 2004

15. Grant, A., Keith; Kaussler, Bernd, *The Battle of Aleppo: External Patrons and the Victimization of Civilians in Civil War*, "Small Wars & Insurgencies", Vol. 31, No. 1, 2020
16. Hewitt, Kenneth, *Proving Grounds of Urbicide: Civil and Urban Perspectives on the Bombing of Capital Cities*, "ACME: An International Journal for Critical Geographies", Vol. 8, No. 2, 2015
17. Lewis, Michael, W., *The Law of Aerial Bombardment in the 1991 Gulf War*, "American Journal of International Law", Vol. 97, No. 3, 2003
18. Marx, J. Andrew, *Detecting Urban Destruction in Syria: A Landsat-Based Approach*, "Remote Sensing Applications: Society and Environment", Vol. 4, 2016
19. Mir, Zeinab; Rabet, Majid; Ahmed, Safdar, *Testimonies of Aerial Bombardment and Communities of Self-Expression*, "Digital War", Vol. 5, No. 1-2, 2024
20. Parks, Hays, W., *Air War and the Law of War*, "The Conduct of Hostilities in International Humanitarian Law", Vol. I, Routledge, 2023
21. Sampaio, Antônio, *Before and After Urban Warfare: Conflict Prevention and Transitions in Cities*, "International Review of the Red Cross", Vol. 98, No. 901, 2016
22. Shaw, Martin, *New Wars of the City: Relationships of Urbicide and Genocide*, in *Cities, War, and Terrorism: Towards an Urban Geopolitics*, Wiley-Blackwell, Malden, Oxford, Carlton, 2004
23. Shwayri, T. Sofia, *Modern Warfare and the Theorization of the Middle Eastern City*, in *Urban Theory Beyond the West: A World of Cities*, Routledge, London&New York, 2012
24. Sossai, Mirko, *The Place of Cities in the Evolution of International Humanitarian Law*, "The Italian Yearbook of International Law Online", Vol. 31, No. 1, 2022
25. Watts, Sean, *Under Siege: International Humanitarian Law and Security Council Practice Concerning Urban Siege Operations*, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479608
26. Wilke, Christiane, *How International Law Learned to Love the Bomb: Civilians and the Regulation of Aerial Warfare in the 1920s*, "Australian Feminist Law Journal", Vol. 44, No. 1, 2018
27. Wilke, Christiane; Doutaghi, Helyeh, *Legal Technologies: Conceptualizing the Legacy of the 1923 Hague Rules of Aerial Warfare*, "Leiden Journal of International Law", Vol. 37, No. 1, 2024
28. Woodward, Rachel, *Narratives of Destruction and Survival: Writing and Reading About Life in Urban War Zones*, "Theory&Event", Vol. 10, No. 2, 2007

Documente

1. Amnesty International, *Syria: Human Slaughterhouse: Mass Hangings and Extermination at Saydnaya Prison, Syria*, https://www.amnesty.org/en/documents/mde24/5415/2017/en/
2. Amnesty International, *Ukraine: Deadly Mariupol Theatre Strike "A Clear War Crime" by Russian Forces – New Investigation*, https://www.amnesty.org/en/latest/news/2022/06/ukraine-deadly-mariupol-theatre-strike-a-clear-war-crime-by-russian-forces-new-investigation/
3. Doctors Without Borders, *"We Are Calling for Respect for Human Life" in Ukraine*, https://www.msf.org/human-dignity-and-life-must-be-respected-besieged-mariupol-ukraine
4. Doctors Without Borders, *Eastern Aleppo Hospitals Damaged in 23 Attacks Since July*, https://www.msf.org/syria-eastern-aleppo-hospitals-damaged-23-attacks-july
5. Evans, Michael, *War and the City in the New Urban Century*, "Quadrant", January 1, 2009, https://quadrant.org.au/magazine/uncategorized/war-and-the-city-in-the-new-urban-century/
6. Human Rights Watch, *Gaza: Israeli Strike Killing 106 Civilians an Apparent War Crime: Governments Should Suspend Arms to Israel, Support ICC Probe*, https://www.hrw.org/news/2024/04/04/gaza-israeli-strike-killing-106-civilians-apparent-war-crime
7. Human Rights Watch, *Russia/Syria: War Crimes in Month of Bombing Aleppo*, https://www.hrw.org/news/2016/12/01/russia/syria-war-crimes-month-bombing-aleppo
8. Human Rights Watch, SITU Research, Truth Hounds, *Beneath the Rubble: Documenting Devastation and Loss in Mariupol*, https://www.hrw.org/feature/russia-ukraine-war-mariupol
9. Human Rights Watch, *Ukraine: New Findings on Russia's Devastation of Mariupol: War Crimes Inquiry Needed into Massive Loss of Civilian Life, Infrastructure*, https://www.hrw.org/news/2024/02/08/ukraine-new-findings-russias-devastation-mariupol
10. *ICRC's Customary International Humanitarian Law Database*, https://ihl-databases.icrc.org/

11. *International Covenant on Civil and Political Rights (1976)*, https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr.pdf
12. International Criminal Tribunal for the former Yugoslavia, *Case No. IT-01-42 (The Prosecutor Vs. Strugar Et Al*, https://cld.irmct.org/assets/filings/Judgement-Strugar.pdf
13. Israeli Government, *Humanitarian Efforts*, https://gaza-aid-data.gov.il/main/
14. Israeli Government, *Swords of Iron – Updated National Talking Points*, https://govextra.gov.il/media/tudhphlu/swords-of-iron-updated-national-talking-points-26-10-23.pdf
15. Ministry of Foreign Affairs of Israel, *Hamas-Israel Conflict 2023: Key Legal Aspects*, https://www.gov.il/BlobFolder/news/hamas-israel-conflict2023-key-legal-aspects/en/English_Documents_Hamas-Israel%20Conflict%202023%20-%20Some%20Factual%20and%20Legal%20Aspects%20-%20Israel%20Ministry%20of%20Foreign%20Affairs%20(2%20NOV%202023).pdf
16. TASS Russian News Agency, *Nationalists Use Civilians as Human Shield in Kharkov Region - Russian Defense Ministry*, May 6, 2022, https://tass.com/defense/1448157
17. TASS Russian News Agency, *Putin Declares Beginning of Military Operation in Ukraine*, February 24, 2022, https://tass.com/politics/1409329
18. TASS Russian News Agency, *Russian Aerospace Forces Destroy over 10 Terrorist Strongholds in Syria Killing 50 Gunmen*, February 24, 2016, https://tass.com/defense/858644
19. *The Additional Protocols to the Geneva Conventions (1977)*, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf
20. *The European Convention on Human Rights (1953)*, https://www.echr.coe.int/documents/d/echr/convention_ENG
21. *The Geneva Conventions of 1949*, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf
22. *The Hague Convention of 1899*, https://docs.pca-cpa.org/2016/01/1899-Convention-for-the-Pacific-Settlement-of-International-Disputes.pdf
23. *The Hague Convention of 1907*, https://ihl-databases.icrc.org/assets/treaties/195-IHL-19-EN.pdf
24. *The Rome Statute of the International Criminal Court (1998)*, https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf
25. *The Universal Declaration of Human Rights (1948)*, https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf

Web Sources

1. http://muse.jhu.edu/
2. https://govextra.gov.il/
3. https://ihl-databases.icrc.org/
4. https://papers.ssrn.com/
5. https://quadrant.org.au/
6. https://tass.com/
7. https://www.amnesty.org/
8. https://www.echr.coe.int/
9. https://www.hrw.org/
10. https://www.icc-cpi.int/
11. https://www.icrc.org/
12. https://www.msf.org/
13. https://www.ohchr.org/
14. https://www.thealeppoproject.com/
15. ttps://cld.irmct.org/
16. ttps://docs.pca-cpa.org/

Kamila REZMER
Adam Mickiewicz University of Poznań, Poland

PROTEST POLICING AS A MEANS OF RESTRICTING FREEDOM OF ASSEMBLY DURING THE PANDEMIC IN BULGARIA[1]

Abstract:	*During the coronavirus pandemic, numerous individual rights and freedoms were restricted. Most often, the right to assembly was restricted due to the increased risk of spreading the virus. First, legal regulations introducing total bans on gatherings or periodic bans and determining the number of people who could take part in them. Limitations depended mainly on risk assessment, number of cases and other measurable indicators. However, the restrictions did not stop people from protesting for issues important to them even during the pandemic. In this situation, the security services also had to take measures to limit the citizens' right to assembly.* *The aim of this study is to analyze the nature of the protests, determine what actions were taken by the security services towards the protesters, and evaluate whether they led to an escalation, silencing, or abandonment of further action on the part of the protesters. This will allow us to answer the question: whether, and if yes, to what extent was protest policing one of the means of restricting the right to assembly? Moreover, what was the nature of the activities of the security services? The analyzed period was July 9, 2020, to April 16, 2021, in Bulgaria due to increased protest of citizens who demanded mainly changes and resignation of the government. In the source analysis, mainly data from ACLED was used.*
Keywords:	**Protest policing; freedom of assembly; pandemic; Bulgaria; pandemic restrictions**
Contact details of the authors:	E-mail: kamila.rezmer@onet.pl
Institutional affiliation of the authors:	**Adam Mickiewicz University of Poznań, Poland**
Institutions address:	Uniwersytetu Poznańskiego 5, Poznań, 61-614, 61 829 6517, wnpid@amu.edu.pl

Introduction

In 2020, the world was gripped by panic, which was related to the emergence of the coronavirus, which not only spread very quickly but was also a previously unknown threat on such a large scale, a new challenge for governments. For this reason, in the initial period, the actions taken by governments were very chaotic and often ill-considered. Only with time do counteracting strategies become more logical and well-thought-out, but they are also regulated through various decisions and introduced legal regulations. Gradually, numerous rights and freedoms of citizens were restricted, which was justified by fear for their health and life[2]. As a result, questions began to arise about the possibility of abusing the restrictions applied by governments and their legality. The researchers noted that the legal regulations introduced due to the pandemic caused, among other things, the acceleration of the militant democracy process[3]. One of the most frequently restricted rights was the right to assembly[4].

[1] This work was supported by the National Science Centre, Poland [grant number 2021/43/B/HS5/00290].

[2] Maciej Skrzypek, *Between neo-militant and quasi-militant democracy: restrictions on freedom of speech and the press in Austria, Finland, and Sweden 2008-2019*, "European Politics and Society", Vol. 24, No. 5, 2023, pp. 552-571; Przemysław Osiewicz, *Limitations to the Right to Freedom of Assembly in Poland during COVID-19 Pandemic: The Case of Women's Strike*, "HAPSc Policy Briefs", Vol. 1, No. 2, 2020, pp. 195–200

[3]Joanna Rak, Roman Bäcker (Eds.), *Neo-militant Democracies in the Post-communist Member States of the European Union*, 2022, Routledge, London and New York; Joanna Rak, *Pandemic-Era Civil Disorder in Post-Communist EU*

In Bulgaria, as in most Member States of the European Union, the right to assembly is regulated by Constitution[1], where Article 43 indicates that all citizens shall have the right to peaceful and unarmed assembly for meetings and demonstrations. This matter is also regulated in the Law on Gatherings, Meetings, and Manifestations[2], indicating that citizens, associations, and political and other social organizations can organize gatherings, meetings, and manifestations. Moreover, Bulgaria is a Part to the 1966 International Covenant on Civil and Political Rights (ICCPR)[3].

This study aims to analyze the nature of the protests, determine what actions the security services took towards the protesters, and evaluate whether they led to an escalation, silence, or abandonment of further action on the part of the protesters. This will allow us to answer the question: whether, and if yes, to what extent was protest policing one of the means of restricting the right to assembly? Moreover, what was the nature of the activities of the security services? The analyzed period is from 9 July 2020 to 16 April 2021 in Bulgaria due to increased protests by citizens, who mainly demanded the government resign from office. The source analysis mostly drew upon data from ACLED (The Armed Conflict Location & Event Data Project).

The article has the following structure: The first part is theoretical and methodological; it describes the research assumptions and research questions. The next part is an analysis that allows to answer the questions presented earlier. The last part is the presentation of the results and their discussion. The article is an introduction to the subject of protest policing and focuses on data only from the indicated database. Its aim is to prepare the foundations for in-depth research on this subject, which can be expanded with additional materials that will allow us to interpret data in relation to specific protests. The analysis I propose is intended to indicate general trends regarding the nature of civil disorder and police activities in a specific period due to its specificity.

Theoretical background and methodological remarks

Collective action transforms into civil disorder, and civil disorder continues and changes over time under two conditions, i.e., the model of protest policing or the selected dimensions of protest policing and the level of police's partisanship during protest policing[4]. The dimensions of protest policing include the extent of police respect and protection of protesters' rights, the degree of police tolerance for community disruption, the nature of communication between police and demonstrators, the extent and manner of arrests as a method of managing demonstrators, and the extent and type of force deployed to control demonstrators[5]. Public order policing, called protest policing, is how police use their authority and capacity to handle protest[6].

Clark McPhail, David Schweingruber, and John McCarthy distinguish between two models of police protest: negotiated management and escalation of force[7]. Joanna Rak proposed that both models, i.e., escalated

---

Member States, Routledge, 2025; Maciej Skrzypek, *Democratic backsliding in Poland on example drafts amendments in electoral code during the COVID-19 pandemic*, "Polish Political Science Yearbook", Vol. 50, No. 2, pp. 37-50

[4] Kamila Rezmer-Płotka, *Policy on Public Assemblies in Times of Crises: Recommendations Concerning the Strategy of Militant Democracy*, "HAPSc Policy Briefs Series", Vol. 1(2), 2020, pp. 201–207; Przemysław Osiewicz, *Limitations to the Right to Freedom of Assembly*; Maciej Skrzypek, *A Hybrid Strategy of Restrictions of Assembly in Modern Militant Democracies. Experiences from Austria, Finland, and Sweden*, "Journal of Comparative Politics", Vol. 15, No. 2, pp. 24-38

[1] *Constitution of the Republic of Bulgaria*, https://www.parliament.bg/en/const (25.10.2024)

[2] *Laws on The Right of Peaceful Assembly Worldwide*, Bulgaria, https://www.rightofassembly.info/country/bulgaria (25.10.2024)

[3] *Idem*

[4] Stephen Reicher, Clifford Stott**,** *Policing the Coronavirus Outbreak: Processes and Prospects for Collective Disorder*, "Policing: A Journal of Policy and Practice", No. 14, No. 3, 2020, p. 569; Julia Hornberger, *We Need a Complicit Police! Political Policing Then and Now*, "SA Crime Quarterly", No. 48, 2014, pp. 17-24

[5] Clark McPhail, David Schweingruber, John D. McCarthy, *Policing Protest in the United States: 1960-1995*, in D. della Porta, H. Reiter (Eds.), in *Policing Protest: The Control of Mass Demonstrations in Western Democracies*, University of Minnesota Press Minneapolis, London, 1998, p. 51

[6] Willem De Lint, *Public Order Policing: A Tough Act to Follow?*, "International Journal of the Sociology of Law", No. 33, No. 4, 2005, p. 180

[7] Clark McPhail, David Schweingruber, John McCarthy, *Policing Protest in the United States: 1960-1995*, in Christian Davenport, Hank Johnston, Carol Mueller (Eds.), *Repression, and Mobilization*, University of Minnesota Press, Minneapolis, pp. 3-32

force[1] and the model known as negotiated management, should be considered two ideal types. The researcher analyzed police behavior on several levels, allowing us to determine a specific situation within which the model of security services' actions can be considered. The first level referred to the protection of individual freedoms. The second level concern is acceptance on the part of the security services for disruptions. The next level is primarily communication between those who protest and the police. The fourth level included arrests, which may be used as a means for disciplining people who protest. The fifth level is the use of violence, which can also be combined with an arrest[2].

It can be assumed, as Jennifer Earl does, that any repressive action against social movements leads to control, constrain, or prevent protest[3]. This means that anything that leads to an escalation of repression against protesters ultimately negatively impacts civil rights and freedoms and restricts them[4]. In this way, the phenomenon of protest policing becomes another means of oppression. The problem becomes more serious when the police protect the political interests of the government, and there is also the politicization of the police[5]. Not only do citizens lose trust in the security services, but at the same time, protests may escalate due to ignoring parts of society with different political views. According to Anne Nassauer, maintaining peace and order during gatherings, including protests, is possible when de-escalating interactions are correctly identified. She indicates that first, it is necessary to focus on communication and effective police management, respect territorial boundaries, avoid escalation signs, and recognize the emotional dynamics of violent outbreaks[6].

This article focuses on the nature of the chosen protests and activities of the security services towards the protesters and whether they led to an escalation, silence, or abandonment of further action on the part of the protesters. It has become possible to answer these questions based on the presented theory and use the qualitative source analysis method. The analyzed data comes from the Covid-19 Disorder Tracker. This database allows the provision of data concerning the dynamics of contention. The protests included in the database are dated from 9th of July 2020 to 16th of April 2021 in Bulgaria due to increased protests by citizens, who mainly demanded the government resign from office. The analysis of the protests was limited to those that occurred in the Bulgarian capital. The purpose of the adopted assumptions and the research is to answer these questions: can protest policing in the analyzed period be treated as one of the means of restricting the right to assembly? Moreover, what was the nature of the activities of the security services?

The study contributes to a better understanding of the consequences of the actions taken by the security services in relation to the protesters. In addition, it indicates the risk associated with treating the police as a means of pursuing the political interests of the government and becoming a means of restricting the rights and freedoms of the individual. This may ultimately lead to a permanent weakening or loss of trust in structures whose primary goal is to protect the life and health of citizens and guarantee security. The conclusions can be used to conduct further extended research regards to protest policing, but civil disorder, too.

Protests in the Bulgarian capital

In 2020, there were 2487 protests. Peaceful demonstrations constituted the majority; as many as 221 protests were of such a nature. There were seven protests with interventions and no information about arrests. However, there were five violent mobilizations. Despite the pandemic, most of the protests referred to demanding the resignation of Prime Minister Borisov and Prosecutor General Geshev. There was also a pro

[1] Karolina Owczarek, *Escalated Force as a Model of Protest Policing: A Case Study of the Rotterdam 2021 protest*, "HAPSc Policy Briefs", Vol. 3, No. 2, 2022

[2] Joanna Rak, *Policing Anti-Government Protests During the Coronavirus Crisis in Poland: Between Escalated Force and Negotiated Management*, "Teorija in Praksa", Vol. 58(SI), 2021, pp. 598-615; Joanna Rak, Karolina Owczarek, *Freedom of Assembly at Stake: The Warsaw Police's Partisanship During Polish Protests in Times of Pandemic*, "Studia Securitatis", Vol. 16, No. 2, pp. 169–180

[3] Jennifer Earl, *Repression and social movements*, in David A. Snow, Donatella della Porta, Bert Klandermans, and Doug McAdam, (Eds.), *The Wiley-Blackwell Encyclopedia of Social and Political Movements*, Blackwell Publishing Ltd., 2013

[4] Rune Ellefsen, *The Unintended Consequences of Escalated Repression*, "Mobilization – An International Quarterly", No. 26, No. 1, 2021, pp. 87-108

[5] William Smith, *The Politics of Protest Policing: Neutrality, Impartiality, and "Taking the Knee"*, "The Harvard Review of Philosophy", Vol. 28, 2021

[6] Anna Nassauer, *Effective crowd policing: empirical insights on avoiding protest violence*, "Policing: An International Journal of Police Strategies & Management", Vol. 38, No. 1, pp. 132-152

and anti-President Radev protest, which was included in this category. Sixteen protests addressed the issue of the pandemic. Fifty-one protests focused on other topics, including one protest about foreign policy and changes in abortion laws in Poland.

In 2021, there were 70 protests, including only one of the gatherings that was described as a violent demonstration because it escalated into a riot. Two of the protests ended with arrests. All other protests were peaceful. Of all the demonstrations, 38 demanded the resign from office of Prime Minister Borisov and Prosecutor General Geshev, five concerned issues related to the pandemic. Twenty-seven protests were concerned with other issues, including one protest about foreign policy, precisely the case of Alexei Navalny[1].

To sum up, the protests from the analyzed period from 9 July 2020 to 16 April 2021, a total of 317 protests took place. Of these, 290 were peaceful; only 15 can be described as violent demonstrations. Protests during which the security services intervened took place 7 times, and five protests were mobilized towards violence. Based on the analyzed database, there were two arrests. In the latter case, other materials should also be considered, such as media reports, because there seem to be more arrests. The nature of the issues raised during the assemblies was mainly, as was pointed out, anti-government protests, which resulted from the adopted time caesura. A total of 218 protests of this nature took place, and, for comparison, 21 took place in comparison with those related to the pandemic. Protests of a different nature took place 78 times and covered, among others, other domestic and foreign policy issues.

What is essential in this case is that in the analyzed period, the protests included in the study took place in the capital of Bulgaria. However, protests also took place in other cities. However, it is the capital that can be considered the most representative example of what the situation in Bulgaria looked like in the analyzed period.

Bulgaria, Sofia	Number of protests	Peaceful demonstrations	Violent demontrations	Protest with intervetion	Mob violence	Arrest
2020	247	221	14	7	5	-
2021	70	69	1	-	-	2
Summary	317	290	15	7	5	2

Table 1. Protests in the capital of Bulgaria between 9th of July 2020 and 16th of April 2021[2]

Bulgaria, Sofia	Anti-government	Pandemic	Other
2020	180	16	51
2021	38	5	27
Summary	218	21	78

Table 2. Nature of protests in the capital of Bulgaria in the period from 9th of July 2020 to 16th of April 2021[3]

Protest policing in Sofia in the period from 9th of July 2020 to 16th of April 2021

Focusing on the most important media messages, the actions taken by the protesters during the analyzed period took several forms. The primary division includes blockades of critical points, buildings, streets, etc.; protests in front of important buildings; vandalism; form of verbal calls for protest; support for citizens in exile; turning to external institutions; cooperation with other protest groups; petitions; organizing into more formal structures; support from academia; performance protests; and confrontations with the police[4]. Based on the analysis of media reports from that period, it was indicated that during the pandemic, the security services mainly used the following actions against protesters: pepper spray, water cannons, arrests of

[1] Civicus Monitor, *Protest Against Tightening of Covid-19 Measures*, https://monitor.civicus.org/explore/protest-against-tightening-covid-19-measures/ (28.10.2024)
[2] *Data from ACLED*, ACLED (Armed Conflict Location and Event Data) (29.10.2024)
[3] *Idem*
[4] Kamila Rezmer-Płotka, *Policing Civil Disorder in Pandemic-Driven Bulgaria*, "Political Life", Vol. 3, 2022, pp. 56-61

protesters, removal of anti-government tent towns of protesters, and violence against protesters[1]. However, these activities covered the entire period of the pandemic.

However, the actions mentioned above were taken throughout the coronavirus pandemic. In this study, the time when anti-government protests were intensified was distinguished. Based on media reports from that period, it was possible to determine the actions taken by the police and divide them into categories such as distribution of counterdemonstrations, arrest, use of force, interaction with protesters, police detention other than persons, elimination of tents towns and protests blockades; locks; imposition of financial sanctions; use of security measures[2]. These actions are acceptable in the case of security services, depending on the degree of threat. The Code of Ethics for Officials of the Ministry of the Interior with Police Functions was created in Bulgaria in connection with the Co-operation program to strengthen the rule of law, specified that the police may use force "only in cases provided by the law, in case of unavoidable necessity, proportionate to the risk, and to a degree, which is necessary to achieve a lawful goal"[3]. This means that security services must continually assess the risk and take only adequate actions.

Based on the data from ACLED analysis, it is possible to distinguish situations when security services took action against protesters. These were situations when protesters attempted to enter the government headquarters building, threw a smoke bomb at the police, threw stones at the GERB headquarters building in Sofia, threw paving stones, firecrackers, eggs, smoke bombs, plastic bottles, and other objects, tried to break police cordons outside government buildings in Sofia, blocked key city intersections in Sofia, and carried prohibited items.

On the basis of media reports and analyzed data, it can be indicated with a high degree of probability that most of the activities on the side of security services were in response to the behavior of the protesters. This does not mean there is any justification for using force or other safety measures such as pepper spray. In this case, doubts arise about assessing the adequacy and legitimacy of the measures used concerning the protesters. However, it cannot be indicated that if the police had failed to act, the protesters would not have committed acts of vandalism on a larger scale. The attempts to get into key buildings and throw objects of various kinds posed a threat to all protest participants. Some of the participants also openly encouraged the use of acts that could be considered violent. At the same time, the article presented figures showing that most of the protests in Bulgaria were peaceful assemblies. Clashes between police and protesters were confirmed, but they were isolated incidents rather than a picture of large-scale actions. This may lead to the conclusion that the protests from 9th of July 2020 to 16th of April 2021 were closer to the ideal type of negotiated management and non-violence.

Conclusions

This article analyzed the nature of the protests, determined the actions the security services took toward the protesters, and evaluated whether these actions led to an escalation, silencing, or abandonment of further action on the part of the protesters. During the analyzed period, most protests were peaceful despite issues that evoked strong emotions.

Based on the available data, it can be assumed that in a situation where violence occurred, the actions of the police were a response to the protesters' behavior. However, when the security services intervened, the protests escalated. Both sides abused violence in such a situation. Many researchers have pointed out that repression is not an effective intimidation means for protesters. It often leads to the use of violence by protesters who have their own goals and want to be heard[4].

The answer to the first research question cannot be given unequivocally. Such many protests in the Bulgarian capital alone indicates that Bulgarians could exercise their right to peaceful assembly to a large extent. However, this does not exclude the possibility that protest policing may be considered as a means of restricting this right. However, this requires an analysis of protests from the period of the so-called first wave

[1] Kamila Rezmer-Płotka, *Freedom of Assembly Enforcement in Bulgaria During the Coronavirus Crisis*, "Bulletin of the Vasyl. Stus Donetsk National University. Series Political", Vol. 7, 2022, pp. 46-51

[2] Kamila Rezmer-Płotka, *Policing Civil Disorder in Pandemic-Driven Bulgaria*, "Political Life", Vol. 3, 2022, pp. 56-61

[3] Refworld.org.pl, *Bulgaria: Code of Ethics for Officials of the Ministry of Interior with Police Functions*, https://www.refworld.org/legal/decreees/natlegbod/2004/en/74137 (29.10.2024).

[4] Torsten Mix, *Lethal Repression of Peaceful Protest in Africa. Why Do (non-) Accountable and Military Regimes Shoo*t, "Student Paper Series", Vol. 15, 2014, https://www.ibei.org/ibei_studentpaper15_71932.pdf (28.10.2024)

of the pandemic, when EU member states introduced the most restrictions restricting individual freedoms. In this case, it would be possible to check, for example, how many protests did not take place due to regulations and how the security services behaved. Based on media reports and figures, it is also challenging to determine the actual degree of violence and to capture the exact moment when it escalated. Media discourse can also be a tool in the hands of those in power and lead to the delegitimization of anti-government protests, which Joanna Rak very well illustrated in the example of Poland [1]. In the example of the same state, when there were women's protests regarding the tightening of abortion laws, it could be observed that National Television was able to take over the role of law enforcement[2]. For this reason, it is worth being very careful in formulating conclusions based on media reports; they can only supplement the data collected by researchers and civil society organizations.

In the Bulgarian case analyzed, the protests of this period led to the end of Borisov's term of office and his formal resignation. This indicates that the mobilization of society was effective, although it lasted a relatively long time. Moreover, most of the protests were peaceful, and those that could be described as violent protests were a small percentage of all. This example could serve as a prelude to further in-depth research into why violent acts in peaceful protests occurred much more often in some Member States than others.

Funding: This work was supported by the National Science Centre, Poland [grant number 2021/43/B/HS5/00290].

Bibliography

Books

1. Davenport, Christian; Johnston, Hank; Mueller, Carol (Eds.), *Repression, and Mobilization*, University of Minnesota Press, Minneapolis, 2005
2. della Porta, Donatella; Reiter, Herbert (Eds.), *Policing Protest: The Control of Mass Demonstrations in Western Democracies*, University of Minnesota Press Minneapolis, London, 1998
3. Rak, Joanna, *Pandemic-Era Civil Disorder in Post-Communist EU Member States*, Routledge, 2025
4. Rak, Joanna; Bäcker, Roman (Eds.), *Neo-militant Democracies in the Post-communist Member States of the European Union*, Routledge, London and New York, 2022
5. Snow, David, A.; della Porta, Donatella; Klandermans, Bert; McAdam, Doug, (Eds.) *The Wiley-Blackwell Encyclopedia of Social and Political Movements*, Blackwell Publishing Ltd., 2013

Studies and Articles

1. de Lint, Willem, *Public Order Policing: A Tough Act to Follow?*, "International Journal of the Sociology of Law", Vol. 33, No. 4, 2005
2. Ellefsen, Rune, *The Unintended Consequences of Escalated Repression*, "Mobilization – An International Quarterly", Vol. 26, No. 1, 2021
3. Hornberger, Julia, *We Need a Complicit Police! Political Policing Then and Now*, "SA Crime Quarterly" Vol. 48, 2014
4. Mix, Torsten, *Lethal Repression of Peaceful Protest in Africa. Why Do (non-) Accountable and Military Regimes Shoo*t, "Student Paper Series", Vol. 15, 2014, https://www.ibei.org/ibei_studentpaper15_71932.pdf
5. Nassauer, Anna, *Effective crowd policing: empirical insights on avoiding protest violence*, "Policing: An International Journal of Police Strategies & Management", Vol. 38(1), 2015
6. Osiewicz, Przemysław, *Limitations to the Right to Freedom of Assembly in Poland during COVID-19 Pandemic: The Case of Women's Strike*, "HAPSc Policy Briefs", Vol. 1, No. 2, 2020
7. Owczarek, Karolina, *Escalated Force as a Model of Protest Policing: A Case Study of the Rotterdam 2021 protest*, "HAPSc Policy Briefs", Vol. 3(2), 2022

[1] Joanna Rak, *Framing enemies by the state television: delegitimization of anti-government protest participants during the first wave of the pandemic in Poland*, "Journal of Contemporary Central and Eastern Europe", Vol. 29 (2-3), pp. 157-175

[2] Kamila Rezmer-Płotka, *Taking Over the Role of Law Enforcement by National Television: The Case Study of Women's Strike Protest in Pandemic-Ridden Poland*, "HAPSc Policy Briefs", Vol. 3, No.2, pp. 14-20

8. Rak, Joanna, *Framing enemies by the state television: delegitimization of anti-government protest participants during the first wave of the pandemic in Poland*, "Journal of Contemporary Central and Eastern Europe", Vol. 29, 2021
9. Rak, Joanna, *Policing Anti-Government Protests During the Coronavirus Crisis in Poland: Between Escalated Force and Negotiated Management*, "Teorija in Praksa~, Vol. 58(SI), 2021
10. Rak, Joanna; Owczarek, Karolina, *Freedom of Assembly at Stake: The Warsaw Police's Partisanship During Polish Protests in Times of Pandemic*, "Studia Securitatis", Vol. 16, No .2, 2022
11. Reicher, Stephen; Stott**,** Clifford, *Policing the Coronavirus Outbreak: Processes and Prospects for Collective Disorder*, "Policing: A Journal of Policy and Practice", Vol. 14, No. 3, 2020
12. Rezmer-Płotka, Kamila, *Freedom of Assembly Enforcement in Bulgaria During the Coronavirus Crisis*, "Bulletin of the Vasyl. Stus Donetsk National University. Series Political", Vol. 7, 2022
13. Rezmer-Płotka, Kamila, *Policing Civil Disorder in Pandemic-Driven Bulgaria*, "Political Life", Vol. 3, 2022
14. Rezmer-Płotka, Kamila, *Policy on Public Assemblies in Times of Crises: Recommendations Concerning the Strategy of Militant Democracy*, "HAPSc Policy Briefs Series", Vol. 1, No. 2, 2020
15. Rezmer-Płotka, Kamila, *Taking Over the Role of Law Enforcement by National Television: The Case Study of Women's Strike Protest in Pandemic-Ridden Poland*, "HAPSc Policy Briefs", Vol. 3, No. 2, 2022
16. Skrzypek, Maciej, *A Hybrid Strategy of Restrictions of Assembly in Modern Militant Democracies. Experiences from Austria, Finland, and Sweden*, "Journal of Comparative Politics", Vol. 15, No. 2, 2022
17. Skrzypek, Maciej, *Between neo-militant and quasi-militant democracy: restrictions on freedom of speech and the press in Austria, Finland, and Sweden 2008-2019*, "European Politics and Society", Vol. 24, No. 5, 2023
18. Skrzypek, Maciej, *Democratic backsliding in Poland on example drafts amendments in electoral code during the COVID-19 pandemic*, "Polish Political Science Yearbook", Vol. 50, No. 2, 2021
19. Smith, William, *The Politics of Protest Policing: Neutrality, Impartiality, and "Taking the Knee"*, "The Harvard Review of Philosophy", Vol. 28, 2021

Documents

1. *Constitution of the Republic of Bulgaria*, https://www.parliament.bg/en/const
2. *Laws on The Right of Peaceful Assembly Worldwide*. *Bulgaria*, https://www.rightofassembly.info/country/bulgaria
3. Civicus Monitor, *Protest Against Tightening of Covid-19 Measures*, https://monitor.civicus.org/explore/protest-against-tightening-covid-19-measures/
4. Refworld.org.pl, *Bulgaria: Code of Ethics for Officials of the Ministry of Interior with Police Functions*, https://www.refworld.org/legal/decreees/natlegbod/2004/en/74137

Websites

1. https://monitor.civicus.org/
2. https://www.ibei.org/
3. https://www.parliament.bg/
4. https://www.refworld.org/

Nicoleta Annemarie MUNTEANU
Lucian Blaga University of Sibiu, Romania

"ROLUL ANALISTULUI DE INTELLIGENCE ÎN CONTEXTUL DEZVOLTĂRII INTELIGENȚEI ARTIFICIALE" ["INTELLIGENCE ANALYST` ROLE IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE` DEVELOPMENT"] BY ANDREEA ALEXANDRA DINCĂ

Abstract:	*The monograph "Intelligence Analyst` Role in the Context of Artificial intelligence` Development" published in 2024 by the Pim Publishing House provides an exploration of the intersection between Artificial Intelligence (AI) and intelligence analysis. In this timely and comprehensive work, the author examines how AI is revolutionizing the intelligence community, from enhancing data collection and processing to shaping the future of national security.* *The growth of data volume and complexity in today's world, particularly in secret services, demands the introduction of advanced technologies like AI to improve the capacity for data collection, analysis, and interpretation—key functions in safeguarding national security. AI has significantly revolutionized intelligence operations, enhancing the speed, accuracy, and efficiency of data processing and analysis. This technological evolution has made AI an indispensable tool in protecting against security threats posed by real or potential adversaries.* *This work highlights the transformative role of AI in intelligence analysis, emphasizing its potential for improving security, enhancing decision-making, and supporting global data initiatives to address pressing societal challenges.*
Keywords:	**Artificial intelligence; intelligence analysis; AI applications; intelligence community; cyber threats**
Contact details of the authors:	E-mail: nicoleta.munteanu@ulbsibiu.ro
Institutional affiliation of the authors:	**Department of International Relations, Political Science and Security Studies, Lucian Blaga University of Sibiu, Romania**
Institutions address:	550324-Sibiu, Calea Dumbrăvii nr. 34, Tel./ Fax: 0040/269/422169

This book presents an exploration of Artificial Intelligence (AI) within the context of intelligence analysis, in the context of the integration of artificial intelligence (AI) in intelligence analysis, highlighting its benefits for national security. AI enhances data collection, processing, and interpretation, enabling quick and efficient analysis. Key points include big data analysis , reflecting the way AI can process vast amounts of data rapidly; natural language processing (NLP) - AI interprets written texts similarly to humans; threat identification related to the machine learning and deep learning technologies help identify threats; automation - AI automates repetitive tasks, saving time for intelligence analysts; prediction of how AI can anticipate future events based on data predictions; anomaly detection and the way algorithms detect anomalies in data, aiding in threat response.

It is structured into four distinct sections that introduce, define, and explore both theoretical and practical aspects of AI integration in intelligence processes "Introduction: Theoretical and Conceptual Framework for Introducing AI in Intelligence Analysis". This section sets the stage by providing a comprehensive overview of the theoretical foundations that underpin the use of AI in intelligence analysis. It addresses the evolution of AI technologies and their potential impact on the intelligence field. The chapter establishes a conceptual framework that supports the reader's understanding of AI's role and significance in this domain; "Definitions and Concepts on AI Development and Integration into Intelligence Analysis". The

chapter delves deeper into the definitions and key concepts surrounding AI, offering a detailed exploration of its development, capabilities, and the mechanisms behind its integration into intelligence analysis. It highlights various AI methodologies, tools, and their relevance to intelligence work. The section provides clarity on technical jargon, making it accessible to a wider audience while still offering depth for those familiar with the field; "Methodology: SWOT Analysis and Comparative Analysis". The methodology section introduces two key analytical frameworks—SWOT (Strengths, Weaknesses, Opportunities, and Threats) and comparative analysis. These tools are utilized to assess the potential benefits and challenges associated with incorporating AI into intelligence practices. This part is particularly valuable as it offers a structured approach to understanding how AI can be both advantageous and problematic in real-world intelligence applications; "Case Studies" - the case studies presented offer practical examples of AI integration into intelligence analysis, showcasing its applications, successes, and challenges. These real-world examples provide concrete evidence of the book's theoretical assertions, adding a practical dimension to the research. By presenting case studies, the author not only reinforces the theoretical discussions but also illustrates the dynamic role AI plays in transforming intelligence processes.

Intelligence Analyst` Role in the Context of the Artificial Intelligence` Development by Andreea Alexandra Dincă provides an exploration of the intersection between Artificial AI and intelligence analysis. In this timely and comprehensive work, the author examines how AI is revolutionizing the intelligence community, from enhancing data collection and processing to shaping the future of national security. The book highlights the transformative potential of AI in intelligence analysis, addressing how AI tools such as machine

learning, natural language processing, and deep learning are reshaping traditional methods of intelligence gathering and interpretation. Andreea Alexandra Dincă offers a detailed analysis of how these technologies can improve the speed, accuracy, and efficiency of intelligence operations, from analyzing large datasets to predicting future events and identifying emerging threats.

Central to the book is the role of the intelligence analyst in this evolving technological landscape. Andreea Alexandra Dincă explores how AI can assist analysts by automating time-consuming tasks, identifying hidden patterns, and offering data-driven insights. However, the book also emphasizes the importance of human expertise in guiding AI tools, ensuring that ethical considerations, security concerns, and critical thinking remain integral to the intelligence process. Drawing on contemporary case studies, the author illustrates the practical applications of AI in intelligence agencies worldwide, providing real-world examples of how AI is enhancing security measures and decision-making capabilities. She also discusses the broader implications of AI in defense and security, offering a strategic perspective on how AI can contribute to national and global security frameworks.

The text also notes that most intelligence services worldwide have adopted AI and machine learning to enhance their security capabilities. AI mimics human functions like reasoning, learning, planning, and creativity, making it a strategic technology with significant benefits for citizens and society. The integration of AI in intelligence operations has revolutionized data processing and analysis, improving speed, accuracy, and efficiency. AI is crucial for addressing modern security threats, which are increasingly complex and require advanced tools and methodologies. Furthermore, the text emphasizes the importance of ethical considerations and respect for fundamental rights in AI applications. Technological innovation is essential for societal development, providing infrastructure support and driving the evolution of humanity. Recent technological advancements have improved intelligence operations, increased efficiency and quality, and enabling specialized solutions in data analysis. AI algorithms are more effective than traditional methods in identifying potential cyber threats. The European Data Strategy aims to make the EU a global data platform, ensuring secure, fair, and competitive access to cloud services and promoting data sharing between businesses and public institutions.

With a focus on both the challenges and opportunities AI presents for the intelligence community, this book could be resource for intelligence professionals, policymakers, and anyone interested in understanding the future of security in an increasingly digital and data-driven world. Through this work, Andreea Alexandra Dincă demonstrates how AI is not just a technological tool but a strategic asset that is reshaping intelligence analysis for the modern age. The book represents a contribution to the literature on AI and intelligence analysis. It combines theoretical perspectives with practical methodologies and real-world case studies. The choice of AI-related analytical tools, such as SWOT and comparative analysis, strengthens the methodological approach, making it highly relevant for professionals in the field of intelligence analysis and AI research.

While theoretical and conceptual discussions are presented, further elaboration on emerging AI technologies in intelligence analysis, such as machine learning and deep learning, could offer readers a deeper understanding of cutting-edge advancements. A broader international perspective, incorporating examples from various global intelligence agencies, might make the book even more comprehensive. This book stands as a resource for scholars, practitioners, and policymakers interested in the intersection of artificial intelligence and intelligence analysis.