

HYBRID THREATS AND ACTIVITIES: MODERN PERCEPTION AND EVOLUTION

Abstract:	<p><i>The constantly changing security environment has recently been influenced by a series of hybrid threats, widely used by various entities, including states, to achieve the proposed objectives. The specific feature, characteristic of the ongoing events, including the war in Ukraine, denotes the merging of hybrid methods and tactics of action with the conduct of active armed operations. In this context, we consider it extremely important to study the forms of manifestation characteristic of hybrid attacks to identify, prevent and counter them.</i></p> <p><i>The use of hybrid methods, often extremely complex, requires combining the efforts of the international community and adopting concrete actions that would contribute to the protection and promotion of true democratic values.</i></p> <p><i>The danger of hybrid threats consists in combining a wide spectrum of tools, such as: disinformation, propaganda, cyber-attacks, use of cyberspace, support and promotion of terrorist forms of operation, frequently externalized through certain crimes of a terrorist nature, interference in the internal affairs of the state, manipulation of opinion public etc.</i></p>
Keywords:	Hybrid threat; hybrid war; disinformation; cyber-attacks; manipulation of public opinion; forms of hybrid threats; detecting; preventing and combating the hybrid threat; terrorist crimes
Contact details of the authors:	E-mail: silivitalie@gmail.com
Institutional affiliation of authors:	Moldova State University, Faculty of International Relations, Political and Administrative Sciences, Department of Political and Administrative Sciences
Institutions address:	Moldova State University, 60 A. Mateevici Str., Chişinău, http://usm.md

Introduction

Hybrid threats represent a complex and multidimensional security challenge. The essence of this category of threats lies in the combination of several conventional and unconventional methods. The evolution and popularity of the concept of hybrid threats can be largely attributed to the involvement of non-state actors, the development of technologies, globalization and the evolution of the forms and methods of confrontation applied in conflicts. So, from a theoretical point of view, hybrid threats can be characterized by the involvement of different types of actors, guided by certain reasons, who apply specific methods and techniques and tend to cause major negative consequences to potential targets.

One of the specific features of hybrid threats concerns the nature of the subjects involved in this activity. Thus, promoters of hybrid attacks can be states, groups or non-state organizations, or a combination of them. States can use hybrid tactics, including propaganda, cyber-attacks, economic pressure, and conventional military force to achieve their strategic goals. Non-state groups or organizations, externalized through terrorist groups or criminal organizations, can also use hybrid tactics, such as: unconventional warfare, the use of propaganda, disinformation, cyber-attacks, etc. The need to carry out multilateral and in-depth studies is important for perceiving the motives and objectives of these actors, but also for the development of effective methods of prevention and countermeasures.

Another important aspect characteristic of hybrid type attacks, to be investigated at a theoretical level, refers to the methods and techniques used in this sense. Thus, hybrid threats can be characterized by their complexity, as they frequently involve several specific tactics and methods, including economic pressure, cyber-attacks, propaganda, disinformation campaigns, and finally the application of conventional military

force. The use of the performance of communication technology, such as social media platforms, offers certain opportunities that facilitate the way subjects of hybrid attacks operate. For this reason, the application of effective countermeasures must focus on a comprehensive approach, which involves the possibilities of several scientific and research fields, as well as applications, such as those related to cyber security, intelligence, and military strategy.

In this context, we consider that hybrid threats, both theoretically and practically, can be characterized by increased complexity. For the correct perception of the essence of the respective phenomenon, a detailed study of the subjects, their reasons and the applied methods and techniques is necessary. Hybrid attacks represent a serious challenge to global, regional, and national security, requiring joint efforts to ensure knowledge of the essence of this phenomenon and the development of effective detection and prevention methods.

The essence of hybrid threats

Hybrid warfare involves the coordinated use of multiple instruments of power, strategically designed to capitalize on specific weaknesses across all aspects of society, resulting in synergistic outcomes. The threat posed by revisionist actors employing hybrid warfare techniques significantly impacts societies, national governments, and multinational institutions alike¹.

A distinctive characteristic of hybrid threats involves the utilization of unconventional tactics and methods, including disinformation and propaganda, cyber-attacks, to influence public opinion and undermine trust in democratic state institutions. These tactics can be applied by both states and non-governmental organizations or groups to achieve their strategic goals. Moreover, the increasing use of social media and digital technologies facilitates the dissemination of false information, making it more difficult to identify and counter those threats.

Hybrid demonstrations can consist of “the extensive utilization of political, economic, informational, humanitarian, and other non-military methods, orchestrated alongside the protest potential of the population, is further bolstered by covert military strategies”².

Hybrid threats can be characterized by several fundamental features:

- They involve the combined deployment of various power instruments to create imbalance by targeting a wide range of vulnerabilities.
- These threats employ a coordinated strategy that leverages both horizontal and vertical escalation axes.
- There's an emphasis on creativity and ambiguity to generate synergistic effects, especially within the cognitive realm.

Actors engaged in hybrid warfare may employ a diverse array of military, political, economic, civilian, and informational (MPECI) instruments of power. These tools are directed at the political, military, economic, social, informational, and infrastructure (PMESII) vulnerabilities of a target system. This approach enables escalation in both vertical and horizontal dimensions, aiming to achieve strategic objectives while complicating or avoiding decisive counteraction³.

The danger of hybrid threats is recognized by the states of the world, measures being taken to ensure protection against this kind of danger.

Thus, among the actions undertaken, the creation of structures specialized in the identification, prevention and combating of hybrid threats can be mentioned. We mention the European Center of Excellence for Combating Hybrid Threats which was established in Helsinki at the initiative of Finland. The aim of the Center is to support the efforts of member states in combating hybrid threats by strengthening civil and military capabilities, improving the resilience of states and their institutions, deepening NATO-EU cooperation in countering hybrid threats, pooling the expertise of practitioners, representatives of the academic environment and the environment business with member states and their institutions⁴.

¹ MCDC *Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. January 2017, p. 3, https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf (10.04.2024)

² Douglas Cantwell, *Hybrid Warfare in the Legal and Strategic Gray Zone*, "Journal of European Security and Defense Issues" Vol. 10, No. 1, 2020. p. 41, https://www.marshallcenter.org/sites/default/files/files/2020-09/pC_V10N1_en_Cantwell.pdf (15.03.2024)

³ MCDC *Countering Hybrid Warfare Project, Understanding Hybrid Warfare*, January 2017, p. 13

⁴ <https://www.mae.ro/node/55174> (04.03.2024)

Definition and specificity of hybrid threats

We endorse the perspective that while definitions of hybrid threats may differ and should adapt to their changing nature, the concept aims to encompass the blend of coercive and subversive activities, conventional and unconventional methods (such as diplomatic, military, economic, and technological means), which can be orchestrated in a coordinated fashion by state or non-state actors to achieve specific goals while staying below the threshold of formally declared warfare. There's typically a focus on exploiting the target's vulnerabilities and creating uncertainty to impede decision-making processes. Extensive disinformation campaigns, leveraging social media to shape the political narrative or to radicalize, recruit, and direct proxy actors, can serve as conduits for hybrid threats¹. Hybrid threats are designed to exploit vulnerabilities within a country and frequently target the undermining of fundamental democratic values and liberties².

The Republic of Moldova also pays increased attention to the aspects of detecting and preventing hybrid attacks. Thus, RM Law No. 299 of 21.12.2017 regarding the approval of the Information Security Concept of the Republic of Moldova, in article 10 defines the notion of a “hybrid security threat as a subversive and/or information operation, conducted or placed under the command of states, non-state entities, organizations, individuals, which aims, specifically, the weaknesses and vulnerabilities of a sovereign, independent and wholesome government”³.

Hybrid threats and risks are also stated in the Decision of the Parliament of the Republic of Moldova no. 134 of 19.07.2018 for the approval of the National Defense Strategy and the Action Plan regarding the implementation of the National Defense Strategy for the years 2018-2022, which provides in article 10 that the set of threats and risks identified following the analysis of the strategic security environment at the international, regional and national level represents interdependent elements of hybrid warfare, a form of expression of new generation warfare.

At the same time, this normative act also offers its own definition of the hybrid threat, namely: hybrid threat - type of threat from a state or non-state adversary (individuals, groups), which uses, combined and in an adaptive manner (fast, dynamic), conventional and non-conventional methods and means (political, military, diplomatic, economic, cybernetic, informational, etc.) to achieve the established objectives. This type of war is distinguished by a specific form of manifestation, one that oscillates between the conventional and unconventional spectrum of war, creating varied effects, difficult to anticipate and counter. At the same time, it is characterized by various actions, from the use of troops without identification marks or covert actions of military and paramilitary troops, to propaganda actions, information warfare and cyber-attacks⁴.

According to specialists, the primary technologies of hybrid threats applied against the security of the Republic of Moldova must be considered in two ways:

- Organizational: Both state and non-state actors employ hybrid threats as dictated by the situation and prevailing conditions.
- Methods and Means: The involved actors utilize both conventional and unconventional means, strategically combined to meet the demands necessary for achieving success⁵.

Characteristic elements of hybrid aggression

The main characteristic element of the hybrid aggression of hostile forces is the apparently legal nature of the actions carried out, which do not fall within the criminal law field, and respectively, for the conduct of

¹ Joint Communication to the European Parliament and the Council, *Joint Framework on countering hybrid threats a European Union response*, Brussels, 6.4.2016 JOIN (2016) 18, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>, p. 2 (02.04.2023)

² *Idem*

³ Legea Nr. 299 din 21.12.2017 privind aprobarea Concepției securității informaționale a Republicii Moldova. Publicată la 16.02.2018, Monitorul Oficial No. 48-57, Art. 122, https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro (22.04.2023)

⁴ Hotărârea Parlamentului Republicii Moldova nr. 134 din 19.07.2018 pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018–2022. Publicată la 03.08.2018 în Monitorul Oficial No. 285-294, Art. 441, https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro (22.04.2023).

⁵ Svetlana Cebotari, *Războiul hibrid. Unele considerațiuni*, ”Revista Militară”, Vol. 1, No. 13, 2015, p. 28

these actions, the aggressor cannot be presented with legal claims, being generated a complex of qualification difficulties and legal regulation both nationally and internationally.

As the result of detailed studies on the "hybrid war", its following characteristic features were identified:

- in the case of a hybrid war, no official declaration of war is made, nor is there an official capitulation;
- hybrid war exploits national vulnerabilities in political, military, economic, social, informational and infrastructure terms;
- it can be initiated and carried out by both states and non-state structures;
- hybrid war can use means of organized crime (corruption, blackmail, etc.) and terrorist actions, assassinations, crimes, other acts committed to disturb public order;
- it exploits legislative loopholes and ambiguities at the international level to disrupt and even prevent decisions, including military ones, by which to react to such attacks;
- it often relies on the speed, volume and ubiquity of digital technology to disseminate information¹.

As we can see, the complex character and the wide spectrum of actions aimed at creating essential difficulties for entire state systems fully argue for the need to pay more attention to this phenomenon. We contend that integrating the expertise of both academic specialists and practitioners, including those from defense and security fields, in such a context is essential.

Referring to the topic under discussion, we consider it necessary to note that the essence of hybrid warfare remains unchanged – the attacker tries to destroy the opponent through covert operations, sabotage, cyber-attacks, disinformation, political propaganda, terror and economic pressure on the enemy².

We consider it important to note that among the specific forms of terrorism that possess features of some terrorist crimes and can be used as tools in the hybrid war are: instigation for theoretical purposes or public justification of terrorism, rounding up of terrorists, training people to commit crimes of terrorism, activities of financing the theory or providing material support for terrorist purposes, knowingly lying about the act of terrorism, organizing paramilitary formations or participating in them, organizing mass disorder, attacks on critical infrastructure objects, etc. Terrorism, being a weapon used by certain actors, has taken on increasingly diverse forms, moving from the category of asymmetric threats to hybrid threats³.

During hybrid attacks, terrorist organizations are strategically integrated into the external and internal affairs of the targeted state. Through targeted attacks, they aim to radicalize specific segments of the population and undermine the credibility of state policies, draws upon itself resources, and in the most vulnerable periods for society acts as a force that ultimately should push the unstable system to a situation of collapse and instability⁴.

By directing terrorist groups to definite targets in certain states, the manipulator gets the opportunity to create an information background that facilitates the inclusion or exclusion of those states in/from any processes and exercises a total influence on the situation. The changing context of world processes, the balance of power globally and the utilization of new means of warfare allow experts today to talk about the phenomenon of new terrorism as an element of the strategy of waging a "hybrid war"⁵.

Evolutionary elements of hybrid activities

Hybrid activities are increasingly prominent in the European security landscape, marked by a rise in concerns such as electoral interference, disinformation campaigns, malicious cyber activities, and attempts to radicalize vulnerable individuals as proxies for hybrid actors. This has turned European security into a complex and contested issue involving both state and non-state actors.

Unlike the straightforward dynamics of the Cold War, where superpowers competed openly, today's security environment is more intricate and potentially hazardous due to hybrid threats. These threats are characterized by their multidimensional nature, unclear links between different actions, and sometimes, an

¹ <https://www.moldova.org/republica-moldova-tinta-a-razboiului-hibrid-explicam/> (15.01.2024)

² <https://www.moldova.org/republica-moldova-tinta-a-razboiului-hibrid-explicam/> (15.01.2024)

³ Iuliana Udriou, *Detectarea timpurie a crizelor hibride de securitate*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2619256 (15.09.2018)

⁴ Анатолий Рудаков, Сергей Устинкин, *Трансформированная идентичность как ресурс международного терроризма и элемент стратегии «Гибридной войны»*, <https://cyberleninka.ru/article/n/transformirovannaya-identichnost-kak-resurs-mezhdunarodnogo-terrorizma-i-element-strategii-gibridnoy-voiny> (12.04.2024)

⁵ *Idem*

inability to verify certain aspects. While hybrid threats fall short of outright hybrid warfare, failure to detect or respond to them adequately can escalate into full-fledged hybrid warfare. For instance, hybrid threats existed even before events like the annexation of Crimea or the emergence of certain geopolitical tensions. They represent a combination of interconnected threats, where discerning the links between them can be challenging but crucial in preventing the escalation to hybrid warfare. It is important to note that the hybrid threats are transnational as well as transregional. Borders do not longer matter.

According to some opinions, hybrid threats blend military and non-military tactics, along with covert and overt actions. These tactics encompass disinformation campaigns, cyber-attacks, economic coercion, deployment of irregular armed groups, and even the use of regular military forces. The goal of these hybrid methods is to create ambiguity and blur the distinctions between wartime and peacetime, aiming to instill uncertainty and doubt in the minds of their targets¹.

The term "hybrid threats" encompasses the methods and tools employed by both state and non-state actors to advance their interests, strategies, and objectives. These methods are diverse and can include influencing information and propaganda, exploiting logistical vulnerabilities such as energy supply pipelines, engaging in economic and trade-related coercion, undermining international institutions to render rules ineffective, conducting terrorist activities, and creating insecurity through incidents like airspace violations or invoking "legitimate interests" in border disputes and immigration issues. Typically, actors resorting to hybrid methods are either weaker states/actors or those avoiding overtly declared warfare. Without resorting to hybrid activities, these actors would struggle to advance their agendas effectively².

Hybrid activities strategically exploit the vulnerabilities of the opponent while aiming to stay below the threshold of war. Nevertheless, these conflicts possess the potential to escalate into warfare that includes conventional military operations³. Hybrid threats are characterized as a blend of coercive and subversive actions, employing both conventional and unconventional methods such as diplomatic, military, economic, and technological measures. These tactics are orchestrated in a coordinated fashion by either state or non-state actors with the aim of achieving goals while deliberately staying below the threshold that would trigger formal warfare. Within the EU, hybrid threats are a significant concern, with critical infrastructures like energy playing a central role in this context⁴. As a whole, "hybrid methods of warfare, including propaganda, deception, sabotage, and other non-military tactics, have a history of being employed to destabilize adversaries."⁵ As a rule, "hybrid attacks are primarily conducted by states, yet non-state actors like terrorist organizations are also becoming increasingly capable due to their access to advanced technology and financial resources, enabling them to execute highly sophisticated cyber-attacks"⁶.

One of the forms of hybrid war outbreak is propaganda conducted to influence or modify human behavior and misinform public opinion about certain events or situations. It is used to promote a political cause or point of view and to change perceptions. Misinformation is false or misleading information which is passed on in good faith. Disinformation is information known to be false and willfully disseminated⁷.

In a geopolitical context, "hybrid war" is a relatively new concept, particularly relevant to special forces operations. This approach merges the practice of intense resistance and threats to international security with insights gained from combating state and non-state extremism. Hybrid war is propelled by both internal forces seeking to weaken or overthrow governments within a state or region, and external forces aiming to support and convert local actors for potential operational support.

The actions of external forces in hybrid warfare include influencing the economy and social spheres, coordinating diplomatic efforts, and orchestrating protest actions. Special Forces, intelligence agencies, criminal groups, information and psychological operations, and the full spectrum of technological innovations are employed to achieve these goals⁸.

¹ https://www.nato.int/cps/en/natohq/topics_156338.htm (14.09.2018)

² <https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/> (14.09.2018)

³ <https://www.anl.gov/tcp/combating-hybrid-threats> (14.09.2018)

⁴ <http://www.ee-isac.eu/hybrid-threats> (14.09.2018)

⁵ https://www.nato.int/cps/en/natohq/topics_156338.htm (14.09.2018)

⁶ <https://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/> (22.03.2019)

⁷ <http://fhs.diva-portal.org/smash/get/diva2:1186265/FULLTEXT01.pdf> (14.09.2018)

⁸ Svetlana Cebotari, *Războiul hibrid. Unele considerațiuni*, "Revista Militară", Vol. 1, No. 13, 2015, p. 25

From a political-military perspective, hybrid warfare encompasses a broad spectrum of actions executed by opponents, involving both military and irregular units while simultaneously engaging civilian components. N. Fraier, a researcher at the Center for Strategic and International Studies, identifies several threats integral to hybrid warfare, including non-standard terrorist attacks and the deployment of advanced technologies superior to conventional military equipment¹.

We live in an era of hybrid influencing, where state and non-state actors challenge countries and institutions perceived as threats, opponents, or competitors to their interests and goals. Hybrid threats involve methods and activities targeting the opponent's vulnerabilities. These vulnerabilities may stem from historical memory, legislation, outdated practices, geostrategic factors (such as logistics, geography, natural resources, and infrastructure), societal polarization, technological disadvantages, and ideological differences. If the objectives of those employing hybrid methods and activities are not met, the situation can escalate into hybrid warfare, where the use of military force and violence will significantly increase. Hybrid threats represent the "power of the weak," and when effectively employed, they can provide substantial advantages to the weaker side and create potential for future conflicts involving military instruments².

Combating hybrid threats requires an all of government and all of society approach, including:

- New policies and doctrine
- Situational awareness of multidimensional, long-term hybrid campaigns
- Heightened civil and military preparedness.
- Innovative resilience and response strategies to mitigate subversive actions³.

Hybrid aggressors can gain confidence from carefully calibrated hostile actions that skirt de facto thresholds, often employing policies of 'plausible deniability'. While these gains may seem fleeting, they can leave lasting impacts and establish hazardous precedents. The capacity of hybrid warfare to sow destabilization within the international system underscores the need for a comprehensive strategic approach response⁴.

Conclusions

In today's interconnected world, the internet links everything, providing attackers with the freedom and resources needed to achieve specific objectives. These objectives often include undermining and destabilizing societies through coordinated efforts such as hacking, digital espionage, spreading fake news on social media, applying economic pressure, or manipulating elections. Frequently, tracing the source of these attacks is difficult or even impossible⁵.

It's crucial to acknowledge that hybrid threats have already demonstrated their effectiveness in achieving their goals. Cyberspace is extensively utilized for various purposes, with particular emphasis on the manipulation of public opinion, shaping perceptions of events through disinformation, interference in political processes, and the mobilization of large groups of people (often referred to as "Twitter revolutions"). These activities underscore the potency of hybrid threats in influencing and destabilizing societies. Manipulation of public opinion through virtual space presents a certain degree of danger, but we believe that it is not the most dangerous form of exteriorization.

In essence, those mentioned have a direct influence on consciousness, conscience, and the way of thinking. Thus, in this situation, a predisposition of the subject to be manipulated can be ascertained, that is, he/she consciously accepts the correctness of the received information, basing on a personal analysis. At the same time, we believe that the efforts of both theorists and practitioners are to be oriented towards the future, to prevent new non-standard forms of manipulation. Here we refer to the influence on the subconscious, the human psyche, which can be directed towards creating stereotypes of behavior in certain situations.

The danger of the stated form lies in the fact that the subject/s of the influence do not perceive that they are manipulated, but only proceeds in the way their subconscious was programmed. In the given situation, the danger of spontaneity of actions or their unpredictability is greatly increased. The manipulated person may at

¹ Svetlana Cebotari, *Războiul hibrid. Unele considerațiuni*, "Revista Militară", Vol. 1, No. 13, 2015, p. 27

² <https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/> (14.09.2018)

³ <https://www.anl.gov/tcp/combating-hybrid-threats> (14.09.2018)

⁴ MCDC Countering Hybrid Warfare Project, *Countering Hybrid Warfare March, 2019*, p. 18 https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf (10.04.2024)

⁵ <https://time.tno.nl/en/articles/how-gaming-can-raise-our-awareness-of-hybrid-threats/> (14.09.2018)

once, without reason, proceed in a predetermined way, voting, exposing, or supporting someone acceptable for the influence beneficiary. Even worse could be the situations where the affected person can commit crimes, including those of terrorist character, or other illegal acts.

Indeed, hybrid threats are not a new phenomenon, but their impact has been significantly amplified by factors like globalization, hyperconnectivity, and digitization. These trends have made hybrid tactics more potent and challenging to address. Therefore, there is a critical need to promote further studies and understanding of this complex and evolving phenomenon.

Bibliography

Books and Articles

1. Cantwell Douglas, *Hybrid Warfare in the Legal and Strategic gray zone*. "Journal of European Security and Defense Issues", Vol. 10, No. 1, 2020
2. Cebotari, Svetlana, *Războiul hibrid. Unele considerațiuni*, "Revista Militară", Vol. 1, No 13, 2015

Studies

1. Joint Communication to the European Parliament and the Council, *Joint Framework on countering hybrid threats a European Union response*. Brussels, 6.4.2016 JOIN (2016) 18, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>
2. MCDC Countering Hybrid Warfare Project, *Understanding Hybrid Warfare*, January 2017 https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf
3. Udroi, Iuliana, *Detectarea timpurie a crizelor hibride de securitate* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2619256
4. Рудаков, Анатолий; Устинкин, Сергей, *Трансформированная идентичность как ресурс международного терроризма и элемент стратегии «Гибридной войны»* <https://cyberleninka.ru/article/n/transformirovannaya-identichnost-kak-resurs-mezhdunarodnogo-terrorizma-i-element-strategii-gibridnoy-voyny>

Documents

1. Legea Nr. 299 din 21.12.2017 *privind aprobarea Concepției securității informaționale a Republicii Moldova*, publicată la 16.02.2018 în Monitorul Oficial Nr. 48-57 art. 122. URL: https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
2. Hotărârea Parlamentului Republicii Moldova nr. 134 din 19.07.2018 *pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018–2022*, publicată la 03.08.2018 în Monitorul Oficial Nr. 285-294 art. 441, https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro

Websites,

1. <http://fhs.diva-portal.org/>
2. <http://www.ee-isac.eu/>
3. <https://intelligence.sri.ro/>
4. <https://time.tno.nl/>
5. <https://www.anl.gov/>
6. <https://www.hybridcoe.fi/>
7. <https://www.mae.ro/>
8. <https://www.moldova.org/>
9. <https://www.nato.int/>