SAFEGUARDING DIGITAL DISSENT. THE PROTECTION OF DIGITAL RIGHTS AS FUNDAMENTAL RIGHTS

Radu-Michael ALEXANDRESCU[1]
https://doi.org/10.54989/stusec.2025.19.02.07

Abstract

This article examines how the transition from analogue to digital dissent has reshaped the strategies, capacities, and vulnerabilities of contemporary civil resistance movements. Building on a mixed theoretical framework that combines classic resource mobilisation theory, Hannah Arendt's conception of power and public space, Castells's network society, Bennett and Segerberg's "connective action," and critical perspectives on surveillance capitalism and digital authoritarianism, the paper advances the hypothesis that digitalisation simultaneously enhances mobilisation while increasing exposure to surveillance and algorithmic control. Methodologically, the study employs a qualitative–comparative case-study design, focusing on two emblematic movements: the Arab Spring (2010–2011) and Euromaidan in Ukraine (2013–2014). Using content analysis of digital protest materials, NGO and international reports, and specialist academic literature, the article explores the role of social media, mobile technologies, and platform infrastructures in enabling rapid mobilization, networked coordination, and transnational diffusion of protest.

The findings are structured on three analytical levels: micro (individual mobilization and personalized participation), meso (network structures, leaderless organization, and platform dependence), and macro (state policies, digital repression, and mass surveillance). Across all three levels, digital dissent appears fundamentally ambivalent: it expands civic power and lowers the barriers to participation while simultaneously generating new vulnerabilities—from predictive profiling and targeted intimidation to shutdowns, disinformation, and dependency on private platforms. The article concludes with normative recommendations for safeguarding digital dissent, including the protection of digital rights as fundamental rights, limiting mass surveillance, preserving net neutrality, increasing platform accountability, and fostering civic tech and international regulatory frameworks. It argues that defending dissent in the digital age is essential to preserving the foundations of democracy and human dignity.

Keywords: digital dissent; civil resistance; networked social movements; surveillance capitalism; digital authoritarianism; Arab Spring; Euromaidan

Introduction

We chose this topic because my research fits directly within the current global debate on the reconfiguration of civil rights and liberties in a context marked by the rise of executive control, digital surveillance, and the shrinking of civic space. The proposed theme - analyzing the transformation of dissent from analog to digital forms - addresses one of the most

[1] Dr. Radu-Michael Alexandrescu is a political scientist at the Parliament Palace, Chamber of Deputies (Romania). he holds a PhD in Political Science from the University of Bucharest. His research focuses on human rights, the European Court of Human Rights, subsidiarity and the margin of appreciation, at the intersection of political science, law and philosophy, alexandrescu.michael@gmail.com

sensitive dimensions of contemporary freedom: the right to expression, association, and protest in an environment under technological and political pressure from digital platforms.

The panel ”Civil Rights and Freedoms” provided the ideal framework for this discussion, as it explores the mechanisms through which both states and private actors may restrict or, conversely, strengthen the exercise of civil liberties, either through legal regulation or technological infrastructures. My research contributes to these debates through a comparative analysis of the dynamics of power and civic vulnerabilities in the digital space, highlighting the paradox of modern dissent: the same technology that enables public participation can also be instrumentalized for control and censorship. Therefore, the proposed paper complemented the panel's directions by offering an interdisciplinary perspective on the relationship between rights, technology, and civic action, and by emphasizing the need to reinterpret the protection of fundamental freedoms in the age of algorithmic governance.

In the past two decades, there has been a global decline in civil liberties and civic space, marked by the rise of authoritarian tendencies and the restriction of protest rights[1]. This context justifies a close examination of how dissent - opposition to power and the challenge of political order - has adapted from the analog era to the digital age. Analog dissent refers to traditional forms of civil resistance developed in the absence of the internet: from street protests, strikes, and samizdat (the clandestine dissemination of written materials), to what James C. Scott theorized as the “weapons of the weak” - small everyday subversive acts such as feigned compliance, passive resistance, or sabotage. By contrast, digital dissent encompasses new modes of contestation that utilize information technologies: from social media campaigns and hashtag-driven online activism to hacktivism and flash mobilizations enabled by smartphones.

This article investigates how the transition from analog to digital dissent has reshaped the strategies and vulnerabilities of civil resistance movements. The central research question is: “How has the shift from analog to digital dissent reshaped the strategies and vulnerabilities of civil resistance movements?” The proposed hypothesis states: “The digitalization of dissent enhances mobilization capacity but increases exposure to surveillance and algorithmic control.” In other words, digital tools expand the power to organize and disseminate protest, yet simultaneously generate new risks related to monitoring and digital manipulation.

Theoretically, the article draws on several conceptual frameworks. From Hannah Arendt's perspective, political power emerges when people act together in a shared public space - this being the essence of civic freedom - while violence stands as its opposite, the destruction of collective power[2]. If in the 20th century that common space was often the public square or the mass media public sphere, in the 21st century it increasingly becomes a digital one: online forums and social media platforms now function as the virtual agora for debate and protest. As John Stuart Mill emphasized as early as 1859, “the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others”[3]. In his liberal logic, individual liberty is the foundational principle of any democratic order, and state intervention is legitimate only to prevent harm to others. In the contemporary context, this distinction becomes crucial for

[1] Yana Gorokhovskaia, Cathryn Grothe, *The Uphill Battle to Safeguard Rights* https://freedomhouse.org/report/freedom-world/2025/uphill-battle-to-safeguardrights#:~:text=Key%20Findings (10.09.2025)

[2] José Parejo, *Reflections on Power, Diplomacy, and Strategic Foresight* https://www.joseparejo-asociadosai.com/insight-3#:~:text=Hannah%20Arendt%3A%20Power%20and%20the,Digital%20Public%20 (29.10.2025)

[3] John Stuart Mill, *On Liberty*, John W. Parker & Son, London, 1859, p. 14

understanding the relationship between digital freedom and algorithmic surveillance, where "protection" invoked by the state or platforms risks becoming a pretext for control and censorship.

Manuel Castells, theorist of the "network society," emphasizes that the transformation of the communication environment directly restructures power relations: new social movements adopt horizontal, network-based, non-hierarchical forms of organization, reflecting the internet's "many-to-many" structure, which is difficult for traditional institutions to control[1]. Castells refers to these digitally connected movements as "a new kind of social movement"[2], highlighting the spontaneity, distributed nature, and lack of formal leadership in recent protests. In line with this, the theory of "connective action"[3] formulated by W. Lance Bennett and Alexandra Segerberg explains the rise of a personalized, digitalized politics in which mobilization relies less on hierarchical organizations and unified ideological frames, and more on informal networks of individuals connected through online platforms who join their efforts through viral messages and shared hashtags. This transition from classical "resource mobilization"[4], centered on formal organizations, leaders, and material resources - to mobilization through decentralized networks represents one of the major structural discontinuities introduced by the digital age.

Nevertheless, the conceptual continuities between the old and the new protest paradigms should not be overlooked. Zeynep Tufekci argues that although social media allow movements to scale up with unprecedented speed and magnitude, they do not fully substitute the organizational foundations on which traditional, analog movements relied. The capacity to mobilize large numbers of participants quickly is counterbalanced by a form of strategic fragility: without stable internal structures, such movements may struggle to respond effectively to sustained or complex challenges. In this sense, the "power and fragility of networked protests" are inseparable - the internet similarly allows networked movements to grow dramatically and rapidly, but without prior building of formal or informal organizational and other collective capacities… There is really power here… However, the tedious work performed during the pre-internet era… helped create the resilience all movements need to survive and thrive in the long term[5]. In turn, Evgeny Morozov warns

[1] Manuel Castells, *Networks of outrage and hope*, Polity Press, Cambridge, 2015, pp. 9-15

[2] *Ibidem*, p. 21

[3] The concept of *connective action* describes the shift from the traditional logic of collective action, based on hierarchical organizations and unified ideological frames, to a form of mobilization specific to the digital age, in which networked communication becomes the main organizational mechanism. Participation takes place through personalized expressions and interactions on online platforms, where individuals connect through viral messages and symbols, such as "We Are the 99%" from the Occupy Wall Street movement; W. Lance Bennett, Alexandra Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politic*s, Cambridge University Press, Cambridge, 2013, pp. 19–54

[4] The concept of resource mobilization refers to the process through which social movements obtain, organize, and use the resources necessary for collective action, whether tangible (money, infrastructure, spaces, media channels) or intangible (time, expertise, social networks). The sources may come from direct beneficiaries (the beneficiary constituency), external supporters (the conscience constituency), or from public and private institutions strategically enlisted. The authors emphasize that resources must not only be possessed but also organized and activated, and that their density and distribution condition the degree of mobilization and the strategies of the movement. The lack of specialized resources restricts the tactical options available (Jo Freeman, *Resource Mobilization and Strategy: A Model for Analyzing Social Movement Organization Actions*, in Mayer Zald, John McCarthy, (Eds.), *The Dynamics of Social Movements*, University Press of America, Lanham, 1988)

[5] Tufekci explains that social networks allow contemporary movements to expand rapidly and at large scale, but without gradually building the organizational capacities and collective experience that made traditional movements resilient. She uses an analogy with climbing Mount Everest: the internet "helps" movements reach spectacular heights, but without the necessary preparation, which makes them vulnerable to "storms", that is, to

against naïve technological optimism: digital tools can empower dissent, but they can just as easily serve surveillance and propaganda. Morozov has emphasized that the major danger in digital capitalism comes from the rise of global communication corporations that mediate the online public sphere. Democratic states tend to "outsource" population monitoring to these companies, thus avoiding direct accusations of censorship. In his view, the moral panics surrounding fake news have diverted attention from the real enemy - the "digital giants" whose business models rely on amplifying sensationalist content that divides the public for profit[1]. Thus, Shoshana Zuboff has conceptualized the emergence of "surveillance capitalism", in which personal data become the raw material for predicting and influencing human behavior for commercial purposes and social control. This new logic, where digital platforms monitor, profile, and informationally manipulate users has profound consequences for dissent: on the one hand, it facilitates mobilization through open access to global communication; on the other hand, it increases protesters' exposure to mass surveillance, algorithmic censorship, and interference by manipulative actors, whether state or private[2]. Finally, the theoretical framework is complemented by the normative perspective of authors such as Rebecca MacKinnon, who emphasizes the global struggle for internet freedom and the need for a "networked consent" - a new pact through which the fundamental rights of online users are protected against growing pressures toward censorship and excessive monitoring[3].

Building on this mixed theoretical foundation (conceptual continuity versus structural rupture), the present article examines the transformation of analog dissent into digital dissent. The following sections present the research methodology, the case studies analyzed, the Arab Spring and the Euromaidan, followed by the results of the comparative synthesis, the discussion of normative implications, and the overall conclusions.

Theoretical Framework

The transition from analog to digital protest can be understood through two complementary perspectives:

(a) conceptual continuities - aspects of civic resistance that remain constant regardless of the era;

(b) structural ruptures - innovations that fundamentally change how contentious movements are organized and how they act.

"Resource Mobilization Theory"**,** formulated by John McCarthy and Mayer Zald[4], represents a classic framework that emphasizes the continuities. According to this view, the success of a social movement depends on its capacity to mobilize resources (human, financial, organizational) and to build stable protest organizations. In the analog era, movements often relied on trade unions, opposition parties, clandestine groups, or religious networks to aggregate diffuse grievances into sustained collective action. The key elements - solidarity, shared objectives, continuous interaction with authorities, and the strategic use of the media of the time - have remained defining features even today.

---

tactical, strategic, or repressive challenges. (Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, New Haven, 2017, Preface, pp. xii–xiii)

[1] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, New York, 2011

[2] Shoshana Zuboff, T., PublicAffairs, New York, 2019, pp. 63-94; pp. 295-333

[3] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Basic Books, New York, 2012, pp. 225 - 250

[4] John McCarthy, Mayer Zald, *Resource Mobilization and Social Movements: A Partial Theory*, "American Journal of Sociology", Vol. 82, No. 6, 1977, pp. 1212 - 1241

Digital protest has not eliminated the need for common purpose and social cohesion: even in the age of social networks, successful movements must cultivate a sense of community and shared purpose (e.g., demands for freedom and justice), much like earlier analog movements. In other words, "the goal of organizing social movements has not changed" - economic opportunity and political voice remain constant aims of dissidents, even if the technical means differ. At the same time, recent theories highlight the structural ruptures brought about by networked communication. Networked collective action describes the new flexible organizational patterns, lacking formal hierarchies, that are characteristic of the concept of "connective action"[1].

Instead of the rigid ideological framework and the charismatic leader typical of twentieth-century movements, we now see polymorphic mobilizations in which people participate through personalized frames (for example, each protester can articulate their own message on social media, tied to a shared cause, without necessarily following a line imposed by an organization). Castells notes that the expansion of digital networks has enabled the emergence of horizontal communication, from many to many, beyond centralized control. Through social networks and messaging applications, dispersed activists can coordinate spontaneous collective actions, replicating the characteristics of the digital environment: speed, viral diffusion, and decentralization. Thus, contemporary protests tend to be "self-convoked" online and then materialize in the occupation of physical spaces (squares, streets) - a form of hybridization between the digital and the physical sphere, as Castells also observes in his analyses of movements such as the "Indignados" and "Occupy"[2]. Empirical studies on the Arab Spring confirm this tendency: the 2011 protests began with a spark on the internet, the message of the uprising spreading rapidly online, after which the "virtual networks materialized in the streets" through massive occupations of public space[3]. A defining feature of these new movements is leaderless activism — the absence of singular leaders and centralized structure. Coordination takes place ad hoc, through the multitude of connections among participants, which gives the movement elasticity and the ability to grow rapidly, but sometimes also a lack of long-term strategic direction (as Tufekci emphasizes).

An important aspect of the digital transformation is the relationship between continuity and change in the way power is contested. On the one hand, the "conceptual continuities" are reflected in the fact that digital dissent, like analog dissent, is grounded in moral "outrage" and collective "hope" (in Castells's terms) as forces that drive change. Collective emotions - anger at injustice, the desire for freedom - continue to serve as the initial catalyst for mobilization[4]. Moreover, the digital sphere does not operate in a vacuum: street protests, hunger strikes, marches, and other offline tactics remain indispensable instruments; they are simply amplified by the online environment (e.g., protest events are organized on Facebook but take place physically). In contrast, the "structural ruptures" emerge at the level of infrastructure and vulnerabilities. Digital dissent unfolds on commercial platforms (Facebook, Twitter, etc.) that did not exist before, and these platforms impose new conditions: they can amplify dissident messages, but they can also algorithmically moderate or censor them.

Digital monitoring also enables authorities to identify and track protesters far more easily than in the analog era. If in the past conspiratorial communication required secret meetings or the covert circulation of pamphlets, today much of activist communication

[1] Lance Bennett, Alexandra Segerberg, *Op cit*., p. 19-54
[2] Manuel Castells, *Op. cit.*, p. 284
[3] *Ibidem*, pp. 105-109
[4] *Ibidem*, pp 1-19; pp. 314-316

occurs openly online, leaving digital traces. This creates an unprecedented exposure to surveillance which our hypothesis highlights as the hidden cost of increased mobilization capacity.

A relevant concept in this regard is the digital divide. As early as 2008, Tara Brabazon warned that not everyone has equal access to the "digital revolution": the assumption that "everyone is online" and can participate in digital dissent is mistaken. Internet access, digital skills, and online freedom vary across social groups and countries, creating inequalities in the ability to engage in digital dissent[1]. Therefore, we can say that analog and digital dissent coexist, influencing one another. For example, those excluded from the online sphere (the elderly, poor communities without internet access) may continue to be "analog dissidents," or, conversely, they may remain marginalized due to the lack of alternative means of expression. At the same time, authoritarian regimes aware of the internet's mobilizing power resort to tactics of forced return to the analog: shutting down the internet and mobile communications during protests, censoring independent websites, and so on[2]. Such "shutdowns" were used, for example, in Mubarak's Egypt in 2011, when blocking digital networks actually had the opposite effect, people gathered in even greater numbers in the streets, relying on traditional social networks (Friday prayers at the mosque, word-of-mouth communication)[3].

In summary, the theoretical framework suggests that digitalization produces a hybridization of dissent: the classic theories of collective mobilization remain relevant (solidarity, organizational resources, and leadership do not disappear, even if they manifest differently), but new paradigms emerge that revolve around networks, platforms, and data. Contemporary movements combine the continuity of goals and values (demands for justice, freedom, human dignity) with innovative tactics and communication channels. This hybridity generates both opportunities (expanded mobilization, transnational connectivity) and dilemmas (organizational fragility, dependence on private infrastructures, digital surveillance). In what follows, we examine these dynamics concretely through two relevant case studies.

Methodology

To investigate the proposed hypothesis, I adopted a qualitative–comparative research design based on the analysis of two major case studies of twenty-first-century civil resistance

[1] In the preface of the volume (pp. xiii–xviii), where Brabazon discusses the myth that "everyone is online" and argues that digitalization has not produced an egalitarian revolution but has instead perpetuated analog injustices; in Chapter 3, "Access Denied: Reading, Writing and Thinking About Techno-Literacy", pp. 3–7, Kathryn Locke directly addresses the concept of the digital divide, the inequality of digital skills, and the exclusion of disadvantaged individuals from the online sphere; and then in Chapter 2, "Restless Redundancy" (pp. 11–19); Sonia Bellhouse examines the digital marginalization of those without internet access, including the elderly, the unemployed, and low-income individuals; Tara Brabazon (Ed.), *The Revolution Will Not Be Downloaded: Dissent in the Digital Age*, Chandos Publishing, Oxford, 2008

[2] "Worldwide, there is a growing trend of States resorting to Internet shutdowns and other censorship measures, such as website blocking and filtering, network throttling, or disruptions to mobile services, particularly during sensitive moments like protests and elections. These measures ultimately stifle the right to freedom of expression, stop the free flow of information, and conceal grave human rights violations." in ***UN: Human Rights Council adopts resolution on human rights on the Internet* https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/#:~:text=Worldwide%2C%20there%20is%20a%20growing,conceal%20grave%20human%20rights%20violations (20.09.2025)

[3] "Like Egypt, Libya quickly cut off all Internet access in hopes of blocking the social media coordination of protests and the transmission of information to the outside world" in Marc Lynch, *The Arab Uprising The Unfinished Revolutions of the New Middle East*, PublicAffairs, New York, 2012, p.112

movements: the Arab Spring (2010–2011) and the Euromaidan (Ukraine, 2013–2014). These cases were selected according to the criterion of contrasting variation and historical relevance. The Arab Spring represents a regional wave of uprisings in which digital technologies were heavily used for mobilization and the diffusion of messages, whereas Euromaidan is a movement concentrated within a single European country (Ukraine), where both activists and the government employed digital tools in an acute confrontation. By comparing these two contexts, we can highlight both common features (e.g., the role of Facebook in organizing) and specific differences (e.g., the response of an authoritarian regime in the Middle East versus that of a hybrid regime in Eastern Europe). The data collection methods included:

Content analysis of media sources and digital materials from the protests: social media posts, hashtags, videos and photographs produced by participants, and online statements of the movements. These data provide insight into the strategy, discourse, and internal dynamics of the protests, as well as the ways in which digital platforms were used.

Reports from non-governmental organizations (NGOs) and international institutions on freedom of expression and the internet (such as Freedom House, Human Rights Watch, the Arab Social Media Report, etc.). These reports supplied information on the level of online censorship, government attempts to shut down the internet, and the degree of digital surveillance exercised during the protest movements. For example, Freedom House documents the record number of internet shutdowns in Arab Spring countries in 2011, reflecting the regimes' fear of the mobilizing power of social media.

Academic literature and bibliographic sources (books and scholarly articles): works by experts such as Philip Howard and Muzammil Hussain ("Democracy's Fourth Wave?"), Zeynep Tufekci ("Twitter and Tear Gas"), Manuel Castells ("Networks of Outrage and Hope"), Hannah Arendt, and others were consulted to interpret the empirical findings. For instance, Howard and Hussain provide concrete data on the role of social networks in Egypt and Tunisia, including surveys of protesters about their use of Facebook. Such sources link factual observations to the theoretical concepts discussed.

Comparative analysis: after collecting data for each case study, a synchronous comparative approach was employed (placing the two cases side by side).

Justification for case selection: the Arab Spring and Euromaidan were chosen because both had a major political impact (regime changes, subsequent civil conflicts) and both became symbols of digital dissent. In Tunisia, Egypt, and Libya, social networks were dubbed "weapons of the revolution", and the term "Facebook revolution" entered journalistic vocabulary. Similarly, Euromaidan has been described as the first protest movement in the post-Soviet space organized predominantly online and through mobile technologies, to the point that the government responded with unprecedented technological countermeasures (as will be detailed). Moreover, both cases illustrate the ambivalence of digital dissent: on the one hand, the possibility of rapidly mobilizing tens of thousands of people (e.g., Kyiv's Maidan square filled in a single night following a Facebook call-to-action)[1]; in Egypt, the first protest "flash mob" on 25 January 2011 was organized online); on the other hand, there was also significant exposure to digital repression (e.g., the Mubarak regime shut down the internet, while in Ukraine the authorities sent intimidating SMS messages to protesters).

The qualitative methodology adopted here carries the inherent limitations of any case-study approach: the conclusions are not necessarily generalizable to all protest movements,

[1] Mahmood Monshipouri, *Information Politics, Protests, And Human Rights in the Digital Age*, Cambridge University Press, New York, 2016, pp. 135-148

yet they offer valuable insights into broader trends. By triangulating sources (media, reports, academic literature) and by employing a comparative approach, we seek to enhance the credibility of the observations. In the following sections, we will briefly present each case study, followed by a comparative synthesis of the findings.

Case Studies

The Arab Spring (2010–2011)

The Arab Spring consisted of a series of popular uprisings that broke out almost simultaneously in several countries across the Middle East and North Africa (Tunisia, Egypt, Libya, Bahrain, Yemen, Syria, among others), united by a common theme: the contestation of corrupt authoritarian regimes. The role of digital technology was evident from the very beginning. In Tunisia, the trigger for the protests was the viral spread on Facebook and YouTube of the images of Mohamed Bouazizi - the young man who set himself on fire in protest against police abuse[1]. This desperate act generated a wave of online indignation that brought together hundreds of thousands of citizens in street protests. The Tunisian regime responded by attempting to censor the internet, but countless young activists mobilized to spread information through alternative networks, using proxies and Virtual Private Networks[2] (VPNs) essentially engaging in a digital cat-and-mouse game with the authorities. The sequence of events in Tunisia was closely followed throughout the Arab world thanks to social media and satellite news channels, producing a rapid contagion effect: protests inspired by the Tunisian revolution erupted in Egypt (January 2011, Tahrir Square), Yemen, Bahrain, and later in Libya and Syria. A common feature across these countries was the massive use of Facebook to create pages and mobilization events (e.g., the now-famous "We Are All Khaled Said" page in Egypt, dedicated to a young man killed by the police, which gathered hundreds of thousands of followers and issued the call for the January 25, 2011 uprising)[3].

Use of digital technologies: social networks (Facebook, Twitter), video-sharing platforms (YouTube), and blogs served as the fundamental infrastructure for collective action during the Arab Spring. Online activism facilitated three essential functions:

1. Information and awareness: protesters used social media to bypass state-controlled mass media and to inform both domestic and international audiences about regime abuses. In Egypt, for example, participants in the Tahrir Square demonstrations reported that Facebook and Twitter provided them with independent sources of news that the Mubarak regime could not easily control. This free flow of information helped create a shared sense of injustice and strengthened the belief that change was possible. More concretely, surveys conducted among Egyptian protesters showed that social networks played a crucial role in individuals' decisions to join the demonstrations, offering details about the time and place of actions and conveying the sense that many others were ready to take to the streets. The likelihood of joining the protest increased significantly with social media use: according to a

[1] Marc Lynch, *Op. cit.*

[2] A Virtual Private Network (VPN) is a digital security tool that enables the establishment of an encrypted communication channel between a device and a public or private network, thereby safeguarding the confidentiality and integrity of data transmissions. Beyond its technical function, the VPN has significant political and legal relevance, as it serves as a mechanism through which individuals can mitigate state or corporate surveillance, preserve the right to privacy, and exercise freedoms such as access to information and freedom of expression in restrictive digital environments. VPNs are commonly used to circumvent censorship, overcome geographically imposed content restrictions, and secure remote access to institutional infrastructures, making them a key instrument in contemporary discussions on digital rights, regulatory governance, and the balance between security and civil liberties.

[3] Mahmood Monshipouri, *Op. cit.*, p. 94

study by Tufekci & Wilson, half of the respondents stated that they had themselves produced or distributed images from the demonstrations on Facebook[1].

2. Organization and coordination: digital platforms functioned as spaces for deliberation and logistical planning. Closed Facebook groups, email discussion lists, and online forums allowed activists to discuss strategies, distribute responsibilities, and decide on next steps, all far more rapidly and without the need for risky physical meetings (under the watch of the secret police). The 2011 protests were characterized by a "leaderless" mobilization, which did not mean the absence of organization but rather a networked form of organization. In Egypt, groups such as the April 6 Youth Movement or pro-democracy blogger networks had been active online for several years, creating social capital and ties that helped translate the virtual network into street mobilization at the critical moment. An illustrative example is the way protests self-coordinated through Twitter: demonstrators used the hashtag #Jan25 (referring to January 25, the day of the Cairo protest), and on the ground, information about police movements or needed supplies was immediately posted on Twitter, forming a horizontal flow of real-time updates. This real-time communication helped protesters react quickly to police actions and maintain control of the occupied squares[2].

3. Solidarity and transnational reach: a striking effect of the digital environment was the connection of movements across different countries. Social media transformed local protests into global causes, both through international media attention and through direct links among activists in various countries. For instance, young Tunisians, Egyptians, and Libyans communicated with one another via Twitter and messaging exchanges, sharing advice on avoiding surveillance or providing emergency medical care to the injured. Researchers observed that digital networks enabled new cross-border connections, allowing the shared narrative of grievances to circulate rapidly from one country to another. The success of the Tunisian revolution served as an inspiration not only through a contagion of emotion, but also in practical terms, activists in neighboring countries learned effective strategies through social media (e.g., how to organize volunteer networks for food and water in occupied squares, how to use VPNs to post once the government blocked the internet, etc.). Live-streamed broadcasts by citizen-journalists on YouTube or other platforms brought images of the uprisings directly to screens around the world, creating external pressure on the regimes and increasing the international legitimacy of the protesters.

Advantages and limitations: the Arab Spring clearly demonstrated the amplifying potential of digital tools: social networks acted as a "digital scaffold" on which a more vigorous civil society was built. Countries with a more robust mobile and internet infrastructure (e.g., Tunisia, Egypt) were also those where regimes proved more vulnerable in the face of massive protests. In contrast, where internet penetration was low (e.g., Yemen) or where the regime managed to maintain "digital silence" (e.g., Syria, which plunged into civil war before a unified online movement could form), mobilization was more difficult. A major advantage of digital dissent in the Arab context was the breaking of the state's monopoly over the information sphere. In countries where traditional media were heavily censored, the internet became an alternative space for dissident voices and marginalized communities. Through blogs and social networks, activists were able to build a parallel public opinion - something impossible in the pre-digital era. Thus, as Howard and Hussain summarize, social media provided new opportunities and tools for social movements to respond to the

[1] Zeynep Tufekci, Christopher Wilson, *Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square*, "Journal of Communication", Vol. 62, No. 2, 2012, pp. 363–379
[2] Marc Lynch, *Op. cit.*, p. 84-86

conditions in their countries[1], enabling the rapid formation of a shared public sense of grievance.

On the other hand, the vulnerabilities of digital dissent also became apparent. A first set of limitations stemmed from the technological countermeasures deployed by the state. Confronted with unprecedented protests, Arab dictators implicitly acknowledged the importance of digital networks by treating them as a direct threat to their power. Between January and March 2011, the governments of Egypt, Libya, and Syria resorted to deliberate shutdowns of the internet and mobile networks - the most extensive disruptions seen up to that point. In Egypt, all internet providers were shut down for several days at the regime's command, and mobile phone networks were suspended in critical areas. Although this tactic caused massive economic losses (Egypt lost roughly USD 90 million in five days of shutdown)[2] and fueled further public anger, it nevertheless created significant coordination challenges for protesters. Deprived of Facebook and Twitter, demonstrators turned to traditional means of gathering (mosques, radio broadcasts, and Al Jazeera, which continued to transmit satellite news about the uprising). This highlights the fact that excessive reliance on digital infrastructure can become a vulnerability: regimes can deactivate it at any time, even if at significant cost[3].

Another vulnerability was digital surveillance and targeted repression. After the revolutions, it became clear that the regimes in Egypt and Tunisia had been using Western technology[4] (e.g., interception software and Deep Packet Inspection tools[5]) to spy on activists' online communications and identify movement leaders. Many bloggers and administrators of Facebook pages were arrested in the early stages of the protests, or even beforehand, indicating that the secret police were actively monitoring networks in search of organizers. Even so, the sheer number of users overwhelmed the state's surveillance capacity, and in cases where regimes attempted to make an example by publicly punishing a few internet users, the effect was often the opposite (the spiral of silence was broken by the online solidarity expressed toward those arrested).

Another limiting factor was the ephemeral and fragmented nature of digital mobilization. Whereas traditional movements often built durable structures (parties, unions) that continued the struggle over the long term, many Arab Spring movements dissipated after the removal of dictators, lacking a coherent organization capable of managing the democratic transition. The power to topple a regime did not automatically translate into the power to build a new one, and this organizational deficit was partly attributed to the decentralized nature of digital protests. Zeynep Tufekci noted that "Facebook revolutions" struggle to move from the cry of protest to negotiations and reforms, lacking recognized legitimate leaders or clearly articulated agendas[6].

---

[1] Philip N. Howard, Muzammil M. Hussain, *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Oxford University Press, Oxford, 2013, pp. 17-20

[2] "During the heat of the protests in Tahrir Square, Mubarak demanded that the internet infrastructure be shut down; the loss to the national internet cost Egypt 4 percent of its annual GDP, or about $90 million dollars from a loss of revenue and global financial transactions.", *Ibidem,* p. 74

[3] *Ibidem*, pp. 68-88

[4] "(…) Egypt's Mubarak also failed to control information networks but, in the end, made a desperate attempt to shut down mobile networks. UK-based Vodafone complied with the Egyptian regime's demands to shut off mobile phones, which officials then used to send orders and misinformation to protesters", *Ibidem*, p. 70

[5] Another example used by the authors in their research, but one that does not fall within the scope of our study "(…) Iran has tested and implemented its own deep-packet inspection software purchased from Nokia", *Ibidem,* p.71

[6] Zeynep Tufekci, Christopher Wilson, *Op. cit*

Egypt provides the tragic example: after Mubarak's overthrow, the fragmented movement allowed power to be taken over by well-organized forces (the Muslim Brotherhood, followed later by the military), while the young pro-democracy activists who had led the online revolt were marginalized. Overall, the case of the Arab Spring illustrates both the liberating potential of digital dissent and the duality of freedom and control. Social media served as tools of empowerment for civil society, but also as battlegrounds onto which regimes shifted their repressive methods (censorship, cyber-surveillance). This ambivalence is also present in the next case study, Euromaidan, though manifested in ways adapted to a different geopolitical context.

Euromaidan (Ukraine, 2013–2014)

Context and description: Euromaidan refers to the pro-European protests that erupted in Ukraine at the end of 2013, after President Viktor Yanukovych's government suspended the signing of the Association Agreement with the European Union. The uprising began in Kyiv on 21 November 2013, when a few hundred young people (mostly students) gathered in Independence Square (Maidan Nezalezhnosti) following a call posted on Facebook by journalist Mustafa Nayyem. He wrote: *"*Enough with the jokes. Who is ready to meet at Maidan this evening? Likes don't matter. Only comments saying 'I'm coming.' If we gather at least a thousand people, we'll organize*"*[1].

Within a few hours, the message had been massively shared and more than a thousand people announced they would attend. This Facebook post is widely regarded as the spark that ignited the Ukrainian revolution. Protesters demanded that the country return to its pro-European course and called for the resignation of the corrupt government. The movement escalated after the night of 30 November, when special police units (Berkut) violently dispersed peaceful demonstrators, injuring dozens of students. Images of bloodied young people circulated virally, triggering widespread public outrage[2]; as a result, the next day tens of thousands of people (including the students' parents and grandparents) took to the streets in Kyiv. The protests continued throughout the winter, occupying Maidan and even forming a permanent encampment with barricades. In January 2014, severe clashes erupted with security forces, and the Yanukovych regime resorted to draconian anti-protest laws. In February 2014, after the escalation of violence that resulted in more than 100 deaths (the so-called "Heavenly Hundred"), President Yanukovych fled the country and the opposition took power. Euromaidan thus ended with the successful removal of the government[3].

Use of digital technologies: Although Ukraine had a more robust civil society and freer mass media compared to the countries of the Arab Spring, the role of digital tools was equally crucial in Euromaidan. Several notable aspects include:

1. Initial mobilization and the online snowball effect: As noted, a single Facebook post initiated the protest, demonstrating the power of social networks to transform diffuse discontent into immediate collective action. As the movement grew, Facebook pages and Twitter hashtags became key tools for spreading calls to protest across the country. The

[1] Andrei Soldatov, Irina Borogan, *Here's how Facebook kicked off Ukraine's Euromaidan revolution* https://www.businessinsider.com/heres-how-facebook-kicked-off-the-euromaidan-revolution-2015-7#:~:text=Nayyem%20posted%20an%20angry%20message,thousand%2C%20we%20will%20organize%20ourselves (20.09.2025)

[2] Bryon J. Moraski, *Social media, Kyiv's Euromaidan, and demands for sovereignty in Eastern Ukraine* in Mahmood Monshipouri (Ed.), *Op. cit.,* p.136

[3] Mychailo Wynnyckyj, *Ukraine's Maidan, Russia's War: A Chronicle and Analysis of the Revolution of Dignityi,* Ibidem Press, Stuttgart, 2019, Chapter 6, Chapter 7

hashtag #Євромайдан (#Euromaidan) was used for coordination and news updates, while Facebook communities such as "Euromaidan SOS**"** quickly emerged.

Euromaidan SOS began as a Facebook group created by volunteers from the Center for Civil Liberties in the early days of the protests, gathering over 10,000 members in a very short time. Initially designed to report missing or detained protesters, the group evolved into a genuine online civil command center: people posted alerts about the movements of the anti-riot police (Berkut) around the city, and administrators asked local residents in those areas to confirm and relay the information further. This use of Facebook - as a horizontal network for disseminating information[1] - allowed protesters to react much more quickly to the authorities' attempts to surprise or disperse them. Digital platforms eliminated the need for a formal organizational infrastructure: shifts at barricades, food supplies, medical care for the injured, and many other tasks were coordinated voluntarily online, without any official institution directing the process. One participant described Euromaidan as "a massive anthill of initiatives", made possible by networked communication that brought together people with diverse skills into a shared effort[2].

2. Relationship between physical space and digital space: in Euromaidan, the connection between the physical occupation of the central square and online activism was extremely close and complementary. The physical square provided the visibility and symbolic power of the resistance (images of crowds waving EU flags in the freezing cold circulated worldwide), while the digital sphere supplied the back-end functions: communication, internal organization, and public outreach.

There was even a stage with sound equipment at the protest site, where opposition party leaders (such as Klitschko and Yatsenyuk) delivered speeches. Yet what proved particularly interesting were the ad hoc ways in which the online and offline spheres interacted. For example, important announcements (about missing persons, urgent needs for medicine, calls for volunteers) were posted on Euromaidan SOS and then broadcast via loudspeaker in the square. Information therefore flowed in both directions: from the field to the online sphere (with eyewitnesses posting real-time updates from the "front"), and from online platforms back to the field (instructions and news amplified via megaphone). We can thus speak of the emergence of a "hybrid civic infrastructure", in which Facebook and mobile phones became just as essential as electric generators or tents on the Maidan.

3. Involvement of online media and the diaspora: One innovation of Euromaidan was the creation by independent journalists of Hromadske TV, an online television channel streaming continuous footage and news from the protests. Funded through crowdfunding, Hromadske TV bypassed the influence of oligarchs over traditional media, becoming an objective voice of the civic movement. Likewise, the Ukrainian diaspora in the West played

[1] Scholars examining the Euromaidan have shown that digital platforms played a crucial role in enabling rapid coordination and spontaneous forms of collective action. Drawing on extensive interviews and survey data, Olga Onuch demonstrates that Facebook functioned as a horizontal communication network through which activists and ordinary citizens disseminated logistical information, coordinated essential tasks, and bridged otherwise disconnected social groups. This fluid online environment not only accelerated the protesters' capacity to respond to state actions but also facilitated a high degree of grassroots self-organization, replacing the need for formal hierarchical structures. In this sense, the dense, decentralized activity observed during Euromaidan captures the way digital media brought together individuals with diverse skills into a shared civic effort. For a synthesis of how Facebook enabled rapid information flows, logistical coordination, and cross-network bridging during Euromaidan, see Olga Onuch, *Facebook Helped Me Do It': Understanding the EuroMaidan Protester 'Tool-Kit*', "Studies in Ethnicity and Nationalism", Vol. 15, No. 1, 2015, pp. 175-177

[2] *Ibidem*, pp. 170-184

an active role online, amplifying the protesters' messages and lobbying foreign governments.[1]

Advantages and limits: A key advantage of digital dissent during Euromaidan was its adaptability and its ability to stay one step ahead of the authorities. Although the Yanukovych regime was not as totalitarian as others, it attempted to adopt harsh deterrence tactics. However, digitally native protesters were faster. When security forces attacked on 30 November, social networks caused Kyiv to fill with people within a few hours, without that instant digital feedback, the authorities might have been able to cover up the incident. One participant noted that the speed of the network caught those in power off guard: *"*The authorities knew where the Euromaidan SOS base was, but the network moved faster than they expected"[2]. Facebook allowed pro-European protesters to gather without relying on institutional infrastructures (parties, NGOs), to "mobilize without formal organization", as one analyst noted. This made the initial repression more difficult, because there was no clear list of organizers who could be pre-emptively arrested[3]. Another advantage was transparency and documentation: through smartphones, protesters recorded every abuse. When unidentified snipers began shooting at the crowd (February 2014), the videos and livestreams provided incontrovertible evidence of the regime's violence, fueling popular outrage and international pressure.[4]

However, Euromaidan also revealed several sinister innovations used by the state to counter digital dissent. The most notorious was the use of cellular surveillance technology to intimidate protesters. On 20 of January 2014, thousands of people present in the area of street clashes in Kyiv received a simultaneous text message from an unknown number stating: *"*Dear subscriber, you have been registered as a participant in a mass disturbance"[5]. The wording was almost identical to that of the new anti-protest laws promulgated that very day which prescribed prison sentences of up to 15 years for participants in "riots." The message was clear: the government wanted to show protesters that it knew exactly who and where they were, implying that anyone who took to the streets was risking their freedom. This was an unprecedented form of digital psycho-terror, essentially a mass threat delivered through technology.

---

[1] David R. Marples, Frederick V. Mills (Eds.), *Ukraine's Euromaidan: Analyses of a Civil Revolution*, Ibidem Press, Stuttgart, 2015; The book is a collective volume, meaning the texts are written by multiple authors (political analysts, sociologists, and experts on Eastern Europe). Each chapter is authored by a different contributor. The author who most directly examines the role of Facebook and hashtags as mobilization tools is most often Olga Onuch, who in other works is also the author of the study *"'Facebook Helped Me Do It': Understanding the Euromaidan Protester 'Tool-Kit'"* (2015), vide supra. She writes about the ways in which Facebook, Twitter, and hashtags such as #Euromaidan were used for: coordination; building collective identity; transmitting real-time instructions; legitimizing participation through social visibility. Studies on the role of social media draw on several core arguments: the initial mobilization triggered by Facebook; the use of hashtags in three languages (#Євромайдан, #Евромайдан, #Euromaidan) to connect global audiences; documentation of Facebook's role in facilitating protest logistics; the use of Twitter for live reporting; the observation that users moved from liking and sharing content to physical participation.

[2] Andrei Soldatov, Irina Borogan, *Here's how Facebook kicked off Ukraine's Euromaidan revolution* https://www.businessinsider.com/heres-how-facebook-kicked-off-the-euromaidan-revolution-2015-7#:~:text=Nayyem%20posted%20an%20angry%20message,thousand%2C%20we%20will%20organize%20ourselves (20.09.2025)

[3] Mychailo Wynnyckyj, *Op. cit.,* Chapter 4. Descent into Violence

[4] *Idem*

[5] *Text messages warn Ukraine protesters they are 'participants in mass riot'*, https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot#:~:text=,participant%20in%20a%20mass%20riot (20.09.2025)

The message produced shock and anger: many realized that their phones had been tracked by logging their presence on Global System for Mobile Communications (GSM) towers around the square. Although mobile operators denied involvement (security services likely used signal-interception devices, such as "fake cell towers")[1], the incident confirmed the vulnerability of protesters to digital surveillance. The intended effect of intimidation failed, those present were already determined to continue protesting, and the message triggered a wave of public outrage and online defiance (thousands of people shared screenshots of the SMS accompanied by ironic comments)[2]. Nevertheless, the incident remains emblematic of how a state can use algorithmic methods to deter dissent: automatically identifying individuals present in a protest zone and sending targeted messages to a specific group. Another repressive digital instrument was the disinformation and propaganda campaign orchestrated online. Social networks were suddenly flooded with armies of "trolls" and fake accounts spreading conspiracy theories.[3] Ukrainian protesters countered these narratives digitally as well, relying on their own network of volunteer media activists: they produced infographics, explanatory videos, and blogs in foreign languages to debunk propaganda, essentially, a battle for reality on the internet, akin to the broader concept of a "competition for control of reality" in the digital age[4].

The relationship with global digital platforms and infrastructure: an important lesson of Euromaidan is the dependence of civic movements on the decisions of Big Tech companies. Although Facebook did not intervene against the protesters (on the contrary, it facilitated communication)[5], the situation could have been very different had social media companies yielded to government pressure to block certain pages or data. Protesters were fortunate that the Yanukovych regime lacked soft power over major Western tech corporations, and that Ukraine's internet infrastructure was too diverse to be entirely shut down (unlike Egypt, where a handful of major providers could be forced to cut access). Nevertheless, Euromaidan demonstrated that if the digital space becomes hostile or insecure, protest becomes vulnerable. Ukrainian activists had to be inventive: once they realized their communications were being monitored, they began using encrypted applications, "including major hotlines, such as Halas, which were crucial to mass mobilization… other initiatives

[1] *Idem,* The shocking mass text message received by protesters, informing them that they had been "registered" at the protest site, revealed the extent to which security services were able to track mobile phones by logging their presence on nearby GSM towers. Although mobile operators denied involvement, analysts argue that security forces likely deployed signal-interception devices such as fake cell towers (IMSI -The International Mobile Subscriber Identity is a unique numerical code stored on the SIM - Subscriber Identity Module - card that allows mobile networks to identify the subscriber and authorize their access to communication services. The IMSI is automatically transmitted to base stations when a mobile phone connects to a cell, which makes it exploitable in contexts of digital surveillance, including through active interception devices such as *IMSI catchers* "fake cell towers" that mimic GSM antennas in order to collect the identities of mobile phones within a given area), illustrating the structural vulnerabilities of digital communications under repressive conditions

[2] Bryon J. Moraski *Op. cit,* pp. 127 -150

[3] Mychailo Wynnyckyj, *Op. cit,* Chapter 1: Introduction and Bryon J. Moraski, *Op. cit.*, p. 146

[4] Anatoliy Gruzd, Ksenia Tsyganova, *Information Wars and Online Activism During the 2013/2014 Crisis in Ukraine: Examining the Social Structures of Pro- and Anti-Maidan Groups, "*Policy & Internet", Vol. 7, No. 2, 2015, pp.122-128, 2015

[5]Bryon J. Moraski, *Op. cit.*, p. 149, "Events in Ukraine over the course of 2013 and 2014, which led to the ouster of President Yanukovych, seem to illustrate many of the arguments that previous scholars have made about the democratizing potential of information technology and social media. These media served as critical tools that the regime's opponents employed to initiate protests as well as sustain them. Moreover, when clashes between the government and protesters turned violent, Facebook pages and Twitter feeds became resources for those wishing to track developments, disseminate information to a larger national and international audience, and even treat the injured."

included an ”SOS button”, a smart phone app that, when pressed, sent text-messages to relatives and/or friends of the sender, notifying them of emergency and providing the sender’s exact coordinates through the Global Positioning System (GPS)”[1].

In conclusion, Euromaidan underscores the same ambivalence**:** digital networks enabled the protest to grow and endure, but they also provided authorities with new tools of attack (such as the mass SMS, an early example of algorithmic authoritarianism). The protesters’ victory came in part because their numbers exceeded the state’s capacity for control, and the human network ultimately prevailed over the repressive technological network, though not without significant human costs.

Results

The comparative analysis of the two case studies, Arab Spring and Euromaidan, largely confirms the research hypothesis and highlights a set of findings at three levels: micro (individual mobilization), meso (networks and organizations), and macro (state policies and surveillance). Overall, the results reveal the ambivalent nature of digital dissent, which simultaneously enhances the power of civic movements and exposes them to new forms of control.

Micro level (individual mobilization and participation): at the individual level, the shift to the digital era has lowered participation barriers and amplified the capacity for instant mobilization. In both the Arab countries and Ukraine, social media acted as a psychological catalyst: individuals who might otherwise have remained passive spectators joined the protests after seeing on Facebook or Twitter that a significant number of fellow citizens shared similar grievances. Exposure to activist messages online created a bandwagon effect, the perception that a person is not alone; we are many, therefore we can succeed.” Studies from Egypt clearly show this: the use of social media significantly increased the likelihood that an individual would go out to protest even on the very first day[2]. In practice, digital platforms served as new sources of information and trust that regimes could not easily filter.

Another micro-level aspect is the personalization of protest motivations. In analog mobilizations, participation was often mediated by group belonging (a union, a party, a church). In digital mobilization, individuals can engage on the basis of highly personal motivations that they express through their own posts or comments (for instance, someone at Euromaidan may have joined not necessarily because of geopolitics, but because a friend was beaten by the police; another person protested corruption; another, poverty, all these voices finding their place online under a unifying hashtag). This fragmentation of personal narratives did not weaken the movement, on the contrary, it allowed many people with diverse concerns to find themselves represented in at least one aspect of the protest. User-generated content (texts, images, protest memes) reflected this diversity, contributing to a culturalization of dissent: protest was no longer only a physical act, but also a discursive and identity-based act carried out online, in which individuals contributed with their own creativity and unique perspectives. At the same time, the micro level also exhibits heightened vulnerabilities. Every individual leaves digital traces, check-ins, photos, friend lists, that can later be used against them by authorities. For example, in Belarus (a case not analyzed here but contextually relevant), many people who posted pro-opposition comments online were

[1] Svitlana Krasynska, Eric Martin, *The Formality of Informal Civil Society: Ukraine’s EuroMaidan*, Vol. 28, 2017, p. 433-440

[2] Zeynep Tufekci, *Op. cit*., p. 27

later identified and arested or interrogated by the regime[1]. Thus, participation in dissent becomes digitally recorded and archived, increasing personal risks.

In traditional analog protests, the anonymity of the crowd provided a certain degree of protection; now, facial recognition in photographs or metadata from communications can expose anyone's involvement. In Euromaidan, the intimidation SMS was precisely an example of micro-level targeting on a macro scale — each individual physically present was targeted directly.[2] This double-sided nature of the digital sphere at the individual level confirms the hypothesis: greater mobilization capacity, but also greater exposure to personalized repression.

Meso level (networks, organization, and movement dynamics): At the network and organizational level, the transition to the digital era has reshaped the internal organization of resistance movements. The case studies show a shift from relatively hierarchical and formalized structures toward flat, networked structures. Both the Arab Spring and Euromaidan were essentially self-organized movements, even though on the ground they also cooperated with formal entities (e.g., in Egypt, the Muslim Brotherhood joined protests initially led online by secular youth[3]; in Ukraine, opposition parties supported the Euromaidan stage[4]).

One key finding is that digital networks partially substituted for formal organizations, providing the functionalities needed to consolidate a movement: discussion forums, channels of communication, informal collective decision-making mechanisms (polls, informal online votes), etc. This democratizes and broadens the decision-making base, leaders emerge from interaction rather than being pre-designated. Moreover, networks enable flexible coalitions: very different individuals and groups can collaborate ad hoc on a digital platform for a shared goal without needing to agree on all ideological details. For example, on Arab Spring digital groups, secular liberals, socialists, and moderate Islamists interacted freely, united by the objective of toppling dictators even though their long-term visions diverged[5]. This elastic cooperation was facilitated by the open character of digital platforms, where messages circulate according to relevance and appeal, not according to the sender's rank.

However, the absence of formal structures can also lead to meso-level disadvantages. One is institutional fragility: digital movements may lack a stable organizational backbone to sustain them in the long run. After the initial enthusiasm fades, the network may disintegrate unless it is strengthened by something durable (a new political party, a registered civic organization, etc.). In both the Arab countries and, to some extent, in Ukraine, the post-

[1] ***Belarus Activists Fined After Posting Protest Photo Online*, https://www.rferl.org/a/belarus-activists-fined-after-posting-photo-online/24818370.html (20.09.2025)

[2] Krishnadey Calamur, *Ukraine Tracks Protesters Through Cellphones Amid Clashes* https://www.capradio.org/news/npr/story?storyid=264537418 (22.09.2025)

[3] "The Muslim Brotherhood was not among the organizers of the January 25, 2011 «Day of Rage» protest, although it did publicize the protest in advance on its website. Secular youth groups organized the event, and although some Brotherhood members participated in demonstrations on January 25-27, it was not until the protest on Friday, January 28 that the Muslim Brotherhood joined in an official capacity. Once the Brotherhood did join, it played an important role in maintaining the momentum of the protests by supplying logistical support, organization, and participants. Members provided water and food for protesters, the first microphone and speaker tower, and a number of times during the protest, established security checkpoints to prevent pro-government forces from entering Tahrir Square. They also posted information about the protests to their websites. After a couple weeks of protests, the Brotherhood agreed—along with other opposition groups—to meet with the newly appointed vice president, Omar Suleiman." in ***Muslim Brotherhood*, https://carnegieendowment.org/posts/2011/10/muslim-brotherhood?lang=en (20.09.2025)

[4] Mychailo Wynnyckyj, *Op. cit.*, Chapter 3

[5] Philip N. Howard, Muzammil M. Hussain, *Op. cit.*, pp. 3-4

victory organizational vacuum proved problematic. In Egypt, for example, the young activists who coordinated the protest on Facebook had no governance plan; after Mubarak's fall, power was captured by older, better-organized groups (the Muslim Brotherhood and the military)[1]. In Ukraine, some leaders of the emerging civil society later entered formal politics (e.g., journalists like Mustafa Nayyem became members of parliament[2]), so the transition from informal networks to the political system was somewhat more successful. Still, many spontaneous Euromaidan initiatives dissolved after the protest because they were not anchored in a persistent structure. In other words, networks excel at dismantling the status quo, but they cannot replace it; institutional construction still requires traditional organizational forms.

Another disadvantage at the network level is dependence on private platforms and algorithms. The movements analyzed operated primarily on platforms like Facebook, Twitter, and YouTube, corporations with their own policies and commercial interests. This means the "rules of the game" can change at any moment without consulting civic actors. For instance, Facebook's algorithms determine which posts appear on users' feeds; an algorithmic shift could drastically reduce the reach of activist content. If an online campaign does not "catch on" algorithmically (does not trend or generate engagement), its message may remain confined. Additionally, accounts can be suspended by platforms (due to errors or malicious mass reporting by opponents). In practice, the mechanisms of the platform itself can be weaponized against dissenters. Another hypothetical example: if Facebook had decided to delete the "Euromaidan SOS" page for allegedly violating community standards (e.g., for posting violent imagery), it would have caused major communication chaos among protesters. This did not happen, but it is a real risk, movements operate on infrastructures they do not control, making them vulnerable to external decisions[3].

On the "connectivity" dimension, the findings also confirm a major advantage of digital-era movements: their rapid scalability and capacity for self-replication. We have seen how the protest model spread from one country to another during the Arab Spring through digitally facilitated imitation. Similarly, hashtags and practices originating in Euromaidan, such as the "occupation of the square", later inspired protests in Belarus (2020). This transportability of movements is a novel phenomenon: digital networks create transnational bridges for activism that simply did not exist before. As Bennett and Segerberg argue, in "connective action" loyalty to the network can become stronger than loyalty to any formal organization, people rally around a global viral cause[4] (e.g., *#JusticeFor…*) rather than around a local group.

This can serve as a powerful engine of global solidarity, but also introduces a new source of volatility: individuals may shift rapidly from one cause to another depending on what goes viral at a given moment.[5]

Macro level (state, political regimes, surveillance, and public policy): at the macro level, the shift toward digital dissent has also forced governments to adapt their strategies,

[1]Eric Trager, *The Unbreakable Muslim Brotherhood: Grim Prospects for a Liberal Egypt*, https://www.washingtoninstitute.org/policy-analysis/unbreakable-muslim-brotherhood-grim-prospects-liberal-egypt (20.09.2025)
[2]Mustafa Nayyem, https://yes-ukraine.org/en/yes-annual-meetings/2017/speakers/mustafa-nayyem, (21.09.2025)
[3] *Violent and Graphic Content*, https://transparency.meta.com/policies/community-standards/violent-graphic-content/ (23.09.2025)
[4] Lance Bennett, Alexandra Segerberg, *Op. cit,* pp. 87-113
[5] *Ibidem.*, pp. 77-80

making state policy toward the internet a crucial component of governance—especially in authoritarian regimes. The findings clearly show that states[1] have become acutely aware of the subversive potential of the internet and have developed a broad repertoire of countermeasures, ranging from hard censorship (shutdowns, blocking of platforms) to soft censorship (online propaganda, disinformation) and extensive surveillance. In effect, we are witnessing what Ronald Deibert calls *"*the great leap forward in remote-control technologies*"*: security agencies now possess unprecedented capabilities to infiltrate citizens' private lives, both en masse and in highly granular ways, facilitated in part by the rise of the digital surveillance industry[2].

In the cases examined, state responses fit squarely within this global trend. Mubarak's Egypt and other Arab autocracies incorporated internet shutdowns into their repertoire of protest-management tools, a clear indication that they perceived digital networks as a threat to regime security. At the same time, manuals of repressive tactics began to include chapters on information warfare—regimes no longer relied solely on brute force in the streets but fought simultaneously on Facebook and Twitter. The phenomenon of "digital authoritarianism," identified in Freedom House reports, captures precisely this development: the adoption by an increasing number of states of the Chinese-style model of extensive censorship and automated surveillance.[3] Practices such as internet shutdowns during protests are explicitly condemned by the United Nations (through resolutions such as the 2018 Resolution 38/7)[4], yet their number continues to rise each year, evidence that many governments prefer to "flip the digital switch" in order to prevent the spread of unrest. A clear macro-level finding is that the digitalization of dissent has prompted a macro-level response of mass surveillance. Whereas in the 1980[s] state security relied on informants and relatively limited analogue interception, today governments can potentially monitor entire populations with the help of big data algorithms. The surveillance capacities of tech capitalism, namely, the large-scale data collection conducted by corporations such as Google and Facebook, have also become a resource for states. Shoshana Zuboff emphasizes that this model is grounded in the idea of predicting and modifying human behavior for profit and control. When these unprecedented capacities for visibility into private life combine with state authority, the danger becomes distinctly totalitarian. Regimes can use data to identify dissidents before they act (predictive profiling), employ facial recognition to track protest leaders wherever they appear, or implant spyware on phones (as Saudi Arabia did with dissidents using the Pegasus software). Deibert documents how governments like the Saudi regime not only censor but also proactively target digital dissidents: "the Lord of the Flies," Saud al-Qahtani, coordinated thousands of fake accounts and even infiltrated employees

[1] Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace*, Signal/Random House, Toronto, 2013, p 18 "States have become adept at content-control regulations… engaging in offensive operations on their own, including disabling opposition websites … and cultivating a climate of fear and self-censorship".

[2] *Ibidem,* p. 15 Deibert argues that we are at a crossroads marked by: "We stand at a precipice where the great leap in human communication and ingenuity that gave us global cyberspace could continue to bind us together or deteriorate into something malign".

[3] Adrian Shahbaz, *The Rise of Digital Authoritarianism* in https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism#:~:text=The%20Rise%20of%20Digital%20Authoritarianism,censorship%20and%20automated%20surveillance%20systems (25.09.2025)

[4]United Nations Human Rights Council, *Resolution adopted by the Human Rights Council, on 5 July 2018, 38/7. The promotion, protection and enjoyment of human rights on the Internet* https://documents.un.org/doc/undoc/gen/g18/215/67/pdf/g1821567.pdf

inside Twitter to obtain data on opponents, subsequently deploying advanced spyware against them.[1]

On the other hand, state responses are far from uniform. In liberal democracies, authorities face stronger constraints on limiting the internet due to pressure from civil society and legal frameworks that protect fundamental rights. Nevertheless, even in these contexts, tendencies to expand surveillance have emerged under the pretext of national security (debates on backdoors in encrypted applications, intelligence agencies monitoring communications, and similar measures). Some analysts speak of the "westernization of censorship"[2] whereby democratic regimes also adopt forms of internet control, for instance, anti–fake news legislation[3] that can be misused against dissenting content[4]. Recent examples - the case of the france law "2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information"[5], which has triggered reactions across society[6]; Regulation (EU) 2021/784[7] on the removal of terrorist content online has triggered significant opposition, as several NGOs (such as EDRi[8]and Human Rights Watch[9]) have warned that the rapid removal mechanisms could lead to excessive monitoring and the over-restriction of legitimate speech; "(…) France was ranked 26th by Reporters without borders (Reporters sans frontières) in its ranking on freedom of press. This position is worrying since it doesn't resemble the democratic values which France claims to embody"[10] - include attempts within the EU to require platforms to remove "extremist" material, a move criticized by digital rights NGOs as potentially excessive censorship.

Another macro-level finding from comparing the cases is that movements benefit significantly from a robust and open digital infrastructure. Countries with high internet penetration and an active online civil society have generated large-scale protests (e.g., Tunisia, Egypt, Ukraine). Countries where the internet was underdeveloped or heavily controlled from the outset (e.g., Syria, where access to social media was restricted) either did

---

[1] Ronald J. Deibert, O*p. cit.* p. 19 "Countries that censor the Internet have usually relied on products and services developed by Western manufacturers: Websense in Tunisia, Fortinet in Burma, SmartFilter in Saudi Arabia, Tunisia, Oman, and the United Arab Emirates."

[2] Freedom House, *The Crisis of Social Media*, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media (25.09.2025)

[3]Reporters Without Borders, *Predators of press freedom use fake news as a censorship tool*, https://rsf.org/en/predators-press-freedom-use-fake-news-censorship-tool (30.10.2025)

[4] Freedom House, *The Pandemic's Digital Shadow*, https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

[5] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559 (25.09.2025)

[6]Mathieu-Robert Sauvé, Alexandre Coutant, *Loi française contre la manipulation de l'information en période électorale et pratiques professionnelles des journalistes face au phénomène des fake news,* "Les Enjeux de l'information et de la communication", No 23,1A, 2023, https://shs.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2023-S1-page-103?lang=fr (25.09.2025)

[7]Official Journal L 172 of the European Union, Vol 64, 2021, chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=OJ:L:2021:172:FULL&from=EN (30.10.2025)

[8]chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.accessnow.org/wp-content/uploads/2021/09/DSA_Joint_Letter_MEPs.pdf, https://edri.org/our-work/warning-the-eus-digital-services-act-could-repeat-terregs-mistakes/ (30.10.2025)

[9] Deborah Brown, *Draft EU Regulation on 'Terrorist Content' Online Threatens Rights. Proposals Risk Undermining Free Speech, Judicial Authority*, https://www.hrw.org/news/2020/11/16/draft-eu-regulation-terrorist-content-online-threatens-rights (30.10.2025)

[10] Asma Koraichi, Arthur Louis, *Freedom of the press in France: the right to information endangered*, https://www.growthinktank.org/en/freedom-of-the-press-in-france-the-right-to-information-endangered/ (30.10.2025)

not experience similar mass mobilizations or saw them suppressed quickly. Howard and Hussain show statistically that information infrastructure -especially mobile phone usage - consistently appears as a key ingredient of successful movements, and that the absence of internet access correlates strongly with their failure.[1] In other words, the digital scaffolding of civil society becomes a predictor of the fragility of authoritarian regimes. These observations confirm the research hypothesis: digitalization amplifies mobilization but also increases exposure to surveillance and algorithmic control. At the micro, meso, and macro levels, we see this dual dynamic at work. Digital dissent is, in essence, ambivalent: it creates new freedoms and opportunities for expression (thus putting oppressive regimes under pressure), yet it simultaneously generates new vulnerabilities that can be exploited (from individual tracking to mass manipulation). Freedom and control grow simultaneously in the digital sphere—a paradox that modern civic movements must learn to navigate.

Normative Implications and Future Directions

The transformations outlined above entail a series of normative implications and public policy recommendations aimed at safeguarding digital dissent and ensuring that technology remains a tool of civic freedom rather than an instrument of oppression. Moreover, the rapid evolution of technology (artificial intelligence, increasingly opaque algorithms) raises new questions regarding the future of civil contestation, calling for clear avenues for further research. This section discusses the main recommendations and perspectives.

1. Protecting digital rights as an extension of fundamental rights: Although the Charter of Fundamental Rights of the European Union guarantees, through Articles 7 and 8[2], the right to privacy and the protection of personal data, and although the GDPR[3] and the Digital Services Act (DSA)[4] provide a substantial framework for user protection, persistent structural vulnerabilities show that fundamental rights today acquire an indispensable digital dimension. International bodies, including the UN Human Rights Council, have repeatedly affirmed the principle that the rights individuals enjoy offline must also be protected online. However, this principle is not fully realized in practice. Existing EU regulations, ranging from the DSA's prohibition on imposing a general monitoring obligation to the transparency and risk-assessment requirements imposed on Very Large Online Platforms (VLOPs), do not uniformly cover essential aspects of freedom of expression and privacy in the digital environment. Significant gaps remain: the protection of online anonymity, the legal status of end-to-end encryption, the safeguards afforded to digital whistleblowers, and the protection of journalistic sources who work with digital data are still insufficiently consolidated and often vulnerable to political or security-driven pressures.

In this context, the objective is not to create radically new rights, but rather to strengthen, harmonize, and ensure the coherent application of existing ones, so that freedom

[1] Philip N. Howard, Muzammil M. Hussain, *Op. cit.* pp. 46-68

[2] EU Charter of Fundamental Rights, *Article 8 - Protection of personal data*, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data (25.09.2025)

[3] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, OJ, L 119, 2016, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[4] European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*, OJ, L 277, 2022, pp. 1–102, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL%3A2022%3A277%3AFULL (25.09.2025)

of expression, freedom of association, and the right to privacy are effectively guaranteed online. This requires clear regulations that protect users, including activists, investigative journalists, and whistleblowers, and allow them to legitimately use pseudonyms, encryption, and other digital security tools without the risk of disproportionate interference. Similarly, the protection of electronic communications should remain a foundational principle, avoiding the introduction of obligations that could lead to generalized surveillance or unjustified restrictions on online anonymity.

2. Limiting mass surveillance and safeguarding online privacy: in line with international human rights jurisprudence, digital surveillance should be the exception rather than the rule. UN Resolution 38/7 (2018) expressed concern about violations of women's rights online and, more broadly, about the trend toward excessive monitoring of online speech. States have a duty to align intelligence practices with human rights standards, any interception or data collection must be proportionate, justified, and subject to judicial oversight. Normatively, explicit bans should be pursued against identifying peaceful protesters through intrusive technological means, except in cases of serious violence. For example, the use of facial recognition technology on footage of peaceful assemblies could be prohibited by law as a violation of the right to anonymity in public space. Likewise, the "digital panopticon" (the network of cameras plus AI software capable of tracking anyone) must be restrained through regulation: smart cameras and data-analysis tools should be subject to human rights impact assessments before deployment.

3. Ensuring net neutrality and equal access to digital infrastructure: for digital dissent to thrive, internet access must be guaranteed, including in times of political crisis. The 2021 UN resolution[1] on digital rights explicitly condemns deliberate internet shutdowns and urges states not to resort to connectivity interruptions or online censorship, even during elections or protests. Consequently, at the national level, legislation should prohibit governments from arbitrarily shutting down the internet. India, for instance (a country with numerous shutdowns in Kashmir), could align its practices with UN standards, in the spirit that the freedom of assembly includes the infrastructure that enables it. Moreover, net neutrality must be preserved: internet service providers should not degrade or prioritize traffic based on content. This ensures that all voices have an equal opportunity to circulate online. The referenced UN resolution made significant progress, being the first to address net neutrality directly[2]. Strengthening national legislation to reflect this principle remains crucial. While the EU has gradually built a robust framework for digital rights earlier regulatory approaches have evolved, and several instruments have been significantly revised. Without clear guarantees in national laws, governments may still attempt to pressure ISPs to throttle or block platforms used by protesters, illustrating how fragile digital freedoms can be in practice.[3]

4. Holding digital platforms accountable and supporting a tech-savvy civil society: major social media and technology companies play a quasi-governmental role in the digital sphere: they set community rules, moderate content, and thus directly shape the

[1] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age,* Report A/HRC/48/31, 2021, https://docs.un.org/en/A/HRC/48/31 (25.09.2025)

[2] OHCHR, *The right to privacy in the digital age: report (2021),* A/HRC/48/31, https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021?utm_ (27.09.2025)

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ, L 119, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (27.09.2025)

expressive space in which dissent operates. Normatively, a co-regulatory framework is needed in which platforms are required to comply with human rights standards. Initiatives such as the UN ”Guiding Principles on Business and Human Rights” and the EU’s ”Digital Services Act” [1]move in this direction. Platforms should:

- ensure transparency regarding how content is moderated and what is removed (to avoid cases in which legitimate protest content is censored as “incitement”),
- provide procedural safeguards for users—for instance, an activist whose account is removed should have the right to appeal the decision and receive a timely response,
- collaborate with civil society in crafting policies (e.g., working groups with digital rights NGOs to improve misinformation-detection algorithms without depriving dissenters of reach).

At the same time, platforms must resist pressure from authoritarian regimes demanding user data or political censorship. For instance, companies like Twitter and Facebook have received requests from governments to shut down “rebellious” accounts; a rights-aligned approach would require platforms to publicly disclose such requests and legally challenge them when they are abusive[2]. The trend of publishing transparency reports is encouraging, as it reveals how many government requests are received and how companies respond. Cases such as Saudi Arabia, where the regime infiltrated Twitter employees and bribed influencers, illustrate the need for platforms to strengthen internal security and protect dissidents’ data.

In parallel, democratic governments and international organizations should support alternative platforms and open-source tools that promote freedom of expression. For example, the development and funding of decentralized social networks (such as Mastodon) or secure messaging apps (Signal, Tor, Psiphon) can offer activists safer channels. The EU Charter of Fundamental Rights implicitly protects the freedom to receive and impart information without interference (Art. 11), which in practice should translate into support for resilient digital infrastructures. Additionally, the “freedom not to be surveilled” should be considered part of the right to privacy, meaning that states should invest in digital literacy initiatives: operational-security training for activists, encryption guides, and workshops raising awareness about risks such as phishing and spyware.

5. International cooperation and global regulation: digital dissent does not respect borders, which means that global solidarity is essential for its protection. The EU through its Charter of Fundamental Rights and its regulatory framework (e.g., the GDPR on data protection or the recent Artificial Intelligence Act) can serve as a model of “human-centered technology governance” Exporting these standards in its external relations (conditioning agreements on guarantee.s of internet freedom, financing tech-oriented NGOs in oppressive states) is a concrete policy direction. At the UN level, resolutions such as 38/7[3] and its

[1] European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*, OJ, L 277, 2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj (27.09.2025)

[2]Tu˘grulcan Elmas, Rebekah Overdorf, Karl Aberer, *A Dataset of State-Censored Tweets*, Proceedings of the Fifteenth International AAAI Conference onWeb and Social Media, Vol. 15, 2021, p.1009; Freedom House, *Privatizing Censorship, Eroding Privacy,* 2015, https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf (28.09.2025); Freedom House, *Freedom on the Net* 2024, https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf (27.09.2025)

[3] Human Rights Council, *Resolution 38/7, The promotion, protection and enjoyment of human rights on the Internet, 5 July 2018*, A/HRC/RES/38/7, https://documents.un.org/doc/undoc/gen/g18/215/67/pdf/g1821567.pdf (22.09.2025)

successors (2021[1], 2022[2]) provide a normative framework: they explicitly condemn Internet shutdown practices, call on states to promote universal access to the internet, and recognize the importance of encryption and digital security for users. The next step is implementation—meaning that global civil society must pressure governments to comply. These international documents can also be invoked by lawyers in national courts when defending protesters who are prosecuted for online speech.

6. Future research directions: AI, algorithms, and global interdependence
Looking ahead, several emerging trends require careful scholarly atten tion:

Artificial intelligence (AI) and dissent ("algorithmic dissent"): on the one hand, AI-powered systems can be deployed by regimes for predictive surveillance (e.g., social-scoring systems like in China, wide-scale facial recognition), chilling dissent even before it materializes, individuals may self-censor if they know they are constantly monitored. On the other hand, the same technologies can empower activists: AI can help expose propaganda (e.g., automated detection of bot networks), support evidence-based activism (analyzing government data to uncover corruption), or even generate creative forms of protest messaging (AI-generated videos, graphics, or campaigns). Yet the risks are equally significant: regimes can weaponize deepfakes to discredit movement leaders (e.g., fabricating compromising footage). "Algorithmic dissent" may also refer to activism aimed directly at resisting oppressive algorithms, movements demanding transparency and fairness in automated decision-making (for example, protests against discriminatory algorithmic systems used in welfare distribution or credit scoring).

The global interdependence of protest movements: As shown, digital activism tends to diffuse transnationally. The globalization of protest is facilitated by the internet, Occupy, Fridays for Future, Black Lives Matter, and other movements became international largely through hashtags. But this also globalizes repression: censorship and surveillance technologies are exported (companies in democratic countries have sold spyware to authoritarian regimes, e.g., Blue Coat, FinFisher), and authoritarian governments increasingly collaborate and justify each other's models[3] (China promotes the notion of "digital sovereignty", the idea that each state should control its segment of the internet). Interdependence implies that the struggle for internet freedom is becoming part of geopolitics: a potential "digital Cold War" between a bloc of free internet and a bloc of controlled internet. Future research should examine the interaction between global networks of digital activism and global networks of authoritarian digital control.

Civil Society 2.0 and new forms of participation: As digital-native generations reach political maturity, dissent may take entirely new forms, for example, decentralized virtual communities such as DAOs (Distributed Autonomous Organizations)[4] that can fund and coordinate activism without any geographic anchor[5]. This raises profound legal questions

[1] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/48/31, 2021, https://docs.un.org/en/A/HRC/48/31 (22.09.2025)
[2] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/51/17, 2022, https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021 (22.09.2025)
[3] Ronald J. Deibert, *Op. cit.,* p.18
[4] World Economic Forum, *Decentralized Autonomous Organizations: Beyond the Hype*, 2022, pp.6-8 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organizations_Beyond_the_Hype_2022.pdf
[5] Quinn DuPont, *Cryptocurrencies and Blockchains*, Polity Press, John Wiley & Sons, Medford, MA, 2019, chapter eight "Decentralized autonomous organizations are blockchain and smart contract systems for human and machine coordination and decision- making. DAOs rely on blockchain technologies to execute code and record transactions and use smart contracts to tie together people, information sources, and algorithmic agents.

(how do you regulate an NGO that is not physically located anywhere, yet operates globally online?). Moreover, the metaverse may emerge as a new arena for both protest and censorship: if substantial parts of social life move into corporate-owned 3D virtual spaces, will we see virtual sit-ins or avatar marches? And how would principles of freedom of assembly apply in such environments?

Immediate Policy Implications: Ensuring the Resilience of the Digital Civic Space

In the short term, public policy must prioritize safeguarding the resilience of the digital civic sphere. This requires investments in digital literacy, equipping citizens with the ability to recognize propaganda, protect their data, and navigate online risks. It also entails encouraging platform pluralism so that societies do n ot become dependent on only two or three dominant tech corporations. Moreover, states should adopt "emergency communication plans" for periods of internet shutdown or crisis, including the development of local mesh networks, community radio systems, and other decentralized infrastructures.

At the international level, policymakers could consider a *"*Convention on Digital Rights*"* - a global treaty that codifies state obligations in cyberspace, akin to a Geneva Convention for the digital realm, aimed at protecting "digital civilians." Another normative dimension concerns the responsibility of foreign technology suppliers.. The United States[1] have begun adding such entities (e.g., NSO Group) to commercial blacklists. Continuing these efforts is vital to prevent further militarization of anti-dissent technologies. Equally important is the role of civic tech. Idealistic developers and civil society innovators create tools that support democracy—platforms for petitions, election monitoring, legislative crowdsourcing, and transparency. These initiatives deserve institutional support, including public funding, as they strengthen the digital democratic sphere and provide constructive avenues for participation, reducing the likelihood that social grievances will erupt violently.

Conclusions

The comparative study of digital dissent during the Arab Spring and the Euromaidan reveals the ambivalent role of new technologies in moments of challenge to state power. Both episodes showed how social networks and mobile communication can catalyze rapid civic mobilization, enabling large-scale protests to be organized in a very short amount of time. Protesters used platforms such as Facebook and Twitter to coordinate, to disseminate real-time images and information about regime abuses, and to formulate a collective discourse of discontent that transcended social or regional differences. Thus, the digital environment facilitated the emergence of a shared civic identity, for example, in Euromaidan, messages centered on civic dignity and human rights united protesters from diverse groups, even though the movement was not initially grounded in nationalism or language. This finding reflects what Bennett and Segerberg call "connective action", that is, contentious action based

---

Since blockchains are decentralized and persistent, DAOs are too. Smart contracts work autonomously by making decisions based on inputs and programmed responses, and DAOs take action through the output of smart contracts. In many cases, DAOs control and manage participants (rather than the other way around) through economic incentives and prohibitions. DAOs, it is believed, are a radical new mechanism for organizational behavior and social interaction, capable of doing away with the messiness of human relationships, legal contracts, and leaky information flows. Moreover, as governments increasingly function like businesses, they too service their constituents with smart contracts, new voting mechanisms, and strong identity services and authentication.

[1] Bureau of Industry & Security Office of Congressional and Public Affairs, Commerce *Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities (30.09.2025)

on the circulation of personalized content through social media, as opposed to traditional collective action relying on pre-defined group identities[1].

At the same time, the analysis shows that digital uprisings do not emerge ex nihilo, nor do they succeed automatically simply because technology exists. The socio-political context and the actions of regimes were decisive. Following Max Weber's theory of the state, defined as the human community that successfully claims the monopoly of legitimate violence over a given territory[2], the events examined can be interpreted as moments of crisis for this monopoly. In both the Arab countries affected by the uprisings and in Ukraine, mass protests directly challenged the state's authority to exercise force. Regimes often responded with brutal repression in an attempt to reassert control, yet it was precisely the manifestly illegitimate character of violence against peaceful citizens that accelerated the erosion of their legitimacy. For example, in Egypt, as the 2011 demonstrations grew, the Mubarak regime resorted to increasingly violent tactics against protesters, resulting in hundreds of injured and killed[3].

Instead of intimidating the population, these actions fueled public anger and further eroded the authority of the state. Similarly, during Euromaidan, the disproportionate use of force, most notably the violent intervention on 30 November 2013 against a group of peaceful students[4], triggered a wave of national outrage; combined with the instantaneous online circulation of images of the repression, this transformed the protest from a small initial gathering into a mass mobilization against the regime. In Weberian terms, the state compromised the successful exercise of its monopoly on legitimate violence at the moment when citizens, digitally connected and united around democratic values, began to contest the authorities' exclusive right to use force. In practice, both the Arab Spring and the Euromaidan functioned as stress tests of state sovereignty, showing that when state violence loses its appearance of legitimacy, power begins to falter. Nevertheless, the findings of the research also underline the complex and ambivalent character of digital dissent. On the one hand, digital tools have amplified the voice of civil society and weakened the informational control of authoritarian regimes. On the other hand, the study demystifies the techno-utopian view according to which mere "Facebook revolutions" would guarantee democratization.

A first warning concerns the risk of overestimating the emancipatory potential of the online sphere. Although social networks facilitated mobilization, they were not the sole cause of the uprisings, factors such as socio-economic frustration, endemic corruption, and the demand for justice were the real drivers, with technology functioning more as an accelerator. As the literature also notes, the Internet does not exist outside state power: revolutions cannot be simply 'tweeted' into success. Numerous social movements born online failed to have any offline impact precisely because they remained confined to digital activism, their messages dissipating in the void without organizational materialization on the ground.

A second warning arises from the structural vulnerabilities of digital platforms. These virtual spaces, initially perceived as free arenas of expression, suffer from problems such as opaque algorithms (which may favor disinformation or extremist speech for commercial gain), excessive centralization (with a few companies dominating global information flows), and a lack of democratic accountability (decisions on content moderation and data collection

[1] *Vide supra*
[2] Max Weber, *The Vocation Lectures*, Hackett Publishing Company, Indianapolis, 2004, p. 33
[3] Marc Lynch, *Op. cit.,* p. 154, e.g. "Activists rushed back to Tahrir, and over the next few days more than forty civilians were killed and thousands wounded."
[4] *Vide supra*

are made by private entities without adequate public oversight). The study confirms[1] that platforms can exercise a quasi-sovereign power over communication due to the automation of content curation: the algorithms used by social networks can suppress or promote certain messages on an unprecedented scale, embedding commercial priorities deep into the public sphere[2].

Moreover, the dominance of a small number of platforms makes it difficult for activists to "escape" the ecosystem they control, allowing both corporations and governments to manipulate online discourse. Authoritarian actors already exploit these vulnerabilities[3]: as Freedom House reports indicate, virtual spaces are today more manipulated than ever, with authorities aggressively promoting their own narratives and deliberately distorting public debate[4]. We thus observe that non-democratic regimes have learned to use technology against protesters, through censorship, digital surveillance, and automated propaganda, thereby undermining the internet's initial emancipatory potential[5].

A third warning highlighted, closely linked to the previous points, is the need for a realistic assessment of the concrete outcomes of these movements. The Arab Spring, for instance, achieved only partial and short-lived successes: Tunisia managed a difficult democratic transition, but other countries either descended into chaos and conflict (Syria, Libya, Yemen)[6]. Euromaidan produced major political changes in Ukraine (the ousting of the corrupt president and a reorientation toward Europe)[7]. Empirical evidence shows that it is far easier to mobilize protests with the help of new media than to secure lasting political outcomes. These observations do not diminish the importance of digital dissent; rather, they place it in a more nuanced register: technology functions as a facilitator and multiplier of popular will, but not as a substitute for strategic organization, leadership, or a favorable institutional context.

Overall, the general conclusions of this research underscore the transformative potential of digital dissent while simultaneously highlighting its limits and dangers. The internet has become a new frontline in the struggle between society and the state, a space in which the very legitimacy of state power is contested. The state's monopoly on the use of force is called into question in an era in which images of governmental abuses circulate globally within seconds, triggering reactions that cannot be controlled through traditional means. Yet the same digital arena can be infiltrated and instrumentalized, enabling states or other actors to deploy new tactics of power consolidation (mass surveillance, algorithmic disinformation). Thus, digital dissent remains a dialectical phenomenon: it generates historic opportunities for transnational civic emancipation (such as online solidarity around

[1] For detailed analyses of the events, see the works consulted for this study.
[2] Jennifer Cobbe, *Algorithmic Censorship by Social Platforms: Power and Resistance*, "Philosophy&Technology", Vol. 34, 2020
[3] Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum*, Terminus Press, Perth, 2008, pp. 25-26
[4] Freedom House, *New Report: Persistent Authoritarian Repression and Backsliding in Democracies Drive 15th Consecutive Year of Decline in Global Internet Freedom* , https://freedomhouse.org/article/new-report-persistent-authoritarian-repression-and-backsliding-democracies-drive-15th#:~:text=,over%20the%20past%2015%20years (14.11.2025)
[5] Adrian Shahbaz, *The Rise of Digital Authoritarianism*, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism#:~:text=Moreover%2C%20its%20companies%20have%20supplied,an%20engine%20of%20human%20liberation (14.11.2025)
[6] Philip N. Howard, Muzammil M. Hussain, *Op. cit.,* pp. 24-25
[7] Mychailo Wynnyckyi, *Op. cit*., Chapter 10, Chapter 11

revolutionary hashtags and the global transmission of democratic values), but also unprecedented challenges related to preserving an authentic civic space in the age of technology.

The phenomenon of digital dissent is evolving rapidly, and the present conclusions open the way toward numerous avenues for future research. First, there is a need to further deepen studies on the factors that explain the success or failure of digital mobilizations. A stronger grounding in comparative empirical data is essential: why have some uprisings fueled by social media (e.g., Tunisia in 2011, Ukraine in 2014) produced tangible political change, while others were suppressed or co-opted? Future research should investigate the contextual conditions (the level of civil society development, divisions within political elites, or the military's stance toward protests) that, alongside the use of technology, determine post-protest trajectories (democratic transition vs. authoritarian backlash). Longitudinal studies tracking the evolution of post–Arab Spring or post-Euromaidan countries could provide insights into how online activism shapes institutions over the long term, for example, the extent to which networks formed during protests remain active in monitoring governance or engaging in civic initiatives after street demonstrations have ended.

Second, an important new research frontier concerns emerging technologies and their impact on the civic sphere. Artificial intelligence (AI), big data, and advanced digital surveillance are poised to fundamentally reshape both citizens' capacity for mobilization and states' ability to control it. As Freedom House also indicates, the future of internet freedom will depend to a large extent on how governments choose to regulate and deploy the next wave of technologies such as AI[1].

Researchers are therefore encouraged to examine a range of possible scenarios: for instance, could AI, through predictive analytics, anticipate and prevent protests? Or, conversely, could activists deploy intelligent algorithms to evade censorship and amplify their messages? Likewise, topics such as the role of blockchain technology and decentralized networks in civic movements warrant closer attention, there is a growing hypothesis that decentralized tools might reduce dependence on large centralized platforms and thus diminish vulnerability to censorship, yet empirical research remains scarce.

A third area requiring further exploration concerns the transnational dimension of digital solidarity. Events such as the Arab Spring demonstrated the presence of an inspirational contagion effect, protesters in one country were swiftly encouraged by the (real or perceived) successes of their neighbors, in a flow of information unconstrained by borders. Similarly, Euromaidan benefited greatly from the intense support of the Ukrainian diaspora and of international online publics. How are these cross-border networks of digital support constituted, and how effective are they in shaping the trajectory of events? These remain open questions. Theorizing concepts such as "transnational digital solidarity" or the "global connective revolution" could be enriched through case studies tracing how actors in other countries (NGOs, hacktivists, global citizens) participate in local protest movements. Furthermore, the role of digital diasporas deserves attention: highly active expatriate communities can function as bridges between local protesters and international audiences, influencing the global narrative surrounding a domestic conflict and even shaping the foreign policies of other states toward the targeted regime.

[1] *Ibidem,* https://freedomhouse.org/article/new-report-persistent-authoritarian-repression-and-backsliding-democracies-drive-15th#:~:text=The%20future%20of%20internet%20freedom,and%20other%20rapidly%20evolving%20technologies (14.11.2025)

Lastly, a fertile field for future research concerns the strategies of digital civic resilience. As authoritarian states refine their arsenal of censorship and surveillance, it becomes vital to understand the tactics that civil society develops in response. Future studies could document activists' tactical innovations: from the creative use of memes and humor to undermine official propaganda, to the migration toward alternative platforms or the construction of autonomous communication channels (mesh networks, online radio, etc.) when the conventional internet is blocked. Moreover, interdisciplinary research bringing together political scientists, sociologists, IT specialists, and legal scholars is necessary to build a comprehensive picture of the phenomenon.

In conclusion, future research directions should aim to deepen our understanding of the interaction between technology, power, and society. Digital dissent, as an object of inquiry, requires new methodological approaches, combining online social-network analysis (big data, platform analytics) with traditional fieldwork (interviews with activists, direct observation). Only through such approaches can we derive predictive insights into where, when, and how digital tools may tip the balance in favor of democratization or, conversely, how they may be neutralized by the forces of the status quo. Ultimately, the future of digital revolutions remains open, and social science has the responsibility to follow its evolution with critical rigor.

Bibliography

Books

1. Bennett, W. Lance; Segerberg, Alexandra, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*, Cambridge University Press, Cambridge, 2013
2. Brabazon, Tara (Ed.), *The Revolution Will Not Be Downloaded: Dissent in the Digital Age*, Chandos Publishing, Oxford, 2008
3. Castells, Manuel, *Networks of Outrage and Hope: Social Movements in the Internet Age*, Polity Press, Cambridge, 2015
4. Deibert, Ronald J., *Black Code: Inside the Battle for Cyberspace*, Signal Books (Random House), Toronto, 2013
5. DuPont, Quinn, *Cryptocurrencies and Blockchains*, Polity Press, Medford (MA), 2019
6. Howard, Philip N.; Hussain, Muzammil M., D*emocracy's Fourth Wave? Digital Media and the Arab Spring*, Oxford University Press, Oxford, 2013
7. Lynch, Marc, *The Arab Uprising: The Unfinished Revolutions of the New Middle East*, PublicAffairs, New York, 2012
8. MacKinnon, Rebecca, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Basic Books, New York, 2012
9. Malcolm, Jeremy, *Multi-Stakeholder Governance and the Internet Governance Forum*, Terminus Press, Perth, 2008
10. Marples, David R.; Mills, Frederick V. (Eds.), U*kraine's Euromaidan: Analyses of a Civil Revolution*, Ibidem Press, Stuttgart, 2015
11. Mill, John Stuart, On Liberty, John W. Parker & Son, London, 1859
12. Monshipouri, Mahmood (Ed.), *Information Politics, Protests, and Human Rights in the Digital Age*, Cambridge University Press, New York, 2016
13. Morozov, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, New York, 2011

14. Tufekci, Zeynep, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, New Haven, 2017
15. Weber, Max, *The Vocation Lectures*, Hackett Publishing Company, Indianapolis, 2004
16. Wynnyckyj, Mychailo, Uk*raine's Maidan, Russia's War: A Chronicle and Analysis of the Revolution of Dignity*, Ibidem Press, Stuttgart, 2019
17. Zald, Mayer N.; McCarthy, John D. (Eds.), *The Dynamics of Social Movements: Resource Mobilization, Social Control, and Tactics*, University Press of America, Lanham, 1988
18. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019

Studies and Articles

1. Cobbe, Jennifer, *Algorithmic Censorship by Social Platforms: power and resistance*, "Philosophy & Technology", Vol. 34, 2020
2. Elmas, Tuğrulcan; Overdorf, Rebekah; Aberer, Karl, *A Dataset of State-Censored Tweets*, "Proceedings of the Fifteenth International AAAI Conference on Web and Social Media", 2021
3. Gruzd, Anatoliy; Tsyganova, Ksenia, *Information Wars and Online Activism During the 2013/2014 Crisis in Ukraine: examining the social structures of pro- and anti-Maidan groups*, "Policy & Internet", Vol. 7, No. 2, 2015
4. Krasynska, Svitlana; Martin, Eric, *The Formality of Informal Civil Society: Ukraine's EuroMaidan*, "VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations", Vol. 28, No. 1, 2017
5. McCarthy, John D.; Zald, Mayer N., *Resource Mobilization and Social Movements: a partial theory*, "American Journal of Sociology", Vol. 82, No. 6, 1977
6. Onuch, Olga, *'Facebook Helped Me Do It': understanding the EuroMaidan Protester 'Tool-Kit'*, "Studies in Ethnicity and Nationalism", Vol. 15, No. 1, 2015
7. Sauvé, Mathieu-Robert; Coutant, Alexandre, *Loi française contre la manipulation de l'information en période électorale et pratiques professionnelles des journalistes face au phénomène des fake news*, "Les Enjeux de l'information et de la communication, Supplément", No 23/1A, 2023
8. Tufekci, Zeynep; Wilson, Christopher, *Social Media and the Decision to Participate in Political Protest: observations from Tahrir Square*, "Journal of Communication", Vol. 62, No. 2, 2012

Documents

1. *UN: Human Rights Council adopts resolution on human rights on the Internet* https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/#:~:text=Worldwide%2C%20there%20is%20a%20growing,conceal%20grave%20human%20rights%20violations
2. EU Charter of Fundamental Rights, *Article 8 - Protection of personal data*, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data
3. European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL%3A2022%3A277%3AFULL

4. European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*, https://eur-lex.europa.eu/eli/reg/2022/2065/oj
5. https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021
6. Human Rights Council, *Resolution 38/7, The promotion, protection and enjoyment of human rights on the Internet, 5 July 2018*, https://documents.un.org/doc/undoc/gen/g18/215/67/pdf/g1821567.pdf
7. Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age,* https://docs.un.org/en/A/HRC/48/31
8. OHCHR, *The right to privacy in the digital age: report (2021)*, https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021?utm_
9. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679, (27.09.2025)
10. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/48/31, 2021, https://docs.un.org/en/A/HRC/48/31
11. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*,
12. United Nations Human Rights Council, *Resolution adopted by the Human Rights Council, on 5 July 2018, 38/7. The promotion, protection and enjoyment of human rights on the Internet*, https://documents.un.org/doc/undoc/gen/g18/215/67/pdf/g1821567.pdf

Websites

1. https://carnegieendowment.org
2. https://edri.org
3. https://freedomhouse.org
4. https://rsf.org
5. https://transparency.meta.com
6. https://www.bis.gov
7. https://www.businessinsider.com
8. https://www.capradio.org
9. https://www.growthinktank.org
10. https://www.hrw.org
11. https://www.legifrance.gouv.fr
12. https://www.rferl.org
13. https://www.theguardian.com
14. https://www.washingtoninstitute.org
15. https://yes-ukraine.org