COGNITIVE WARFARE AND ITS SOCIETAL IMPACT: MANIPULATION, TRUST AND DEMOCRATIC RESILIENCE

Brînduşa Maria Popa[1]

Regional Department of Defense Resources Management Studies, (DRESMARA) / "Carol I" National Defense University, Brasov, Romania

Cognitive warfare has emerged as a defining feature of contemporary conflict, shifting the focus from physical domains to the manipulation of perception, cognition and societal behavior. This conceptual review article examines the societal impact of cognitive warfare, with particular emphasis on mechanisms of manipulation, the erosion of public trust and the implications for democratic resilience, the challenges democratic societies face in responding to cognitive warfare while preserving fundamental rights, particularly freedom of expression. It argues that strengthening societal resilience requires a balanced approach that safeguards democratic values while countering manipulation.

Drawing on interdisciplinary perspectives from political science, security studies and cognitive psychology, the paper analyses how state and non-state actors exploit digital platforms, information ecosystems and psychological vulnerabilities to influence public opinion. Real-world examples, including electoral interference and disinformation campaigns during global crises, illustrate the tangible consequences of such strategies.

The findings suggest that prolonged exposure to cognitive warfare contributes to polarization, declining institutional trust and weakened democratic participation, effects that can be mitigated through media literacy, institutional transparency and adaptive governance while ensuring that countermeasures do not undermine the democratic principles they seek to protect.

Key words: *resilience, communication, disinformation, security, cognitive warfare.*

[1] ORCID ID: 0000-0002-3215-8000, e-mail: bpopa@mapn.ro

1. INTRODUCTION

Increasingly, conflict has been targeting cognition rather than territory, reflecting the rise of cognitive warfare—a form of strategic competition aimed at influencing how individuals and societies interpret reality. Its effects are subtle, cumulative and difficult to attribute, yet profoundly disruptive (Rid, 2020). This approach is part of a broader set of techniques aimed at subversively targeting the deeper structures of any particular institution or the society itself.

Contemporary events such as disinformation campaigns during the COVID-19 pandemic, influence operations related to the war in Ukraine and misleading narratives about migration in Europe demonstrate that modern conflict unfolds in complex information ecosystems, where narratives, emotions and trust are contested (WHO, 2020; European Commission, 2020).

Societal resilience—the ability of individuals, communities and institutions to withstand, adapt and recover from external disruptions—is central in this context. In democratic societies, resilience depends on public trust, access to reliable information and citizens' ability to critically evaluate competing narratives (OECD, 2021). Its development and expansion are essential for resisting such forms of conflict in this century of asymmetric threats.

While these dynamics are increasingly recognised, this article examines the societal impacts of cognitive warfare and its challenges to democracy, arguing that strengthening societal resilience requires strategies that balance protection against manipulation with the preservation of democratic values (Guess, Nagler and Tucker, 2020).

1.1 Methodology

This article adopts a conceptual and non-systematic review approach aimed at synthetising existing interdisciplinary literature to identify patterns, mechanisms and societal impacts of cognitive warfare.

The analysis is based on academic publications, policy reports and institutional documents produced by organizations such as NATO the European Commission, WHO, OECD. No primary data collection was undertaken. Case examples and literature were selected through a non-systematic, but structured review of articles, official reports from NATO, as well as relevant works in the domain prioritizing sources published between 2016 and 2023 to ensure relevance.

The selection process followed a structured, but non exhaustive strategy, prioritizing influential and recent publications. Case examples were included to support conceptual arguments, rather than to provide empirical comparison.

The objective of this approach is not to test hypotheses, but to identify patterns, mechanisms and societal implications of cognitive warfare across different contexts.

2. CONCEPTUAL FRAMEWORK

Cognitive warfare encompasses strategies aimed at influencing perceptions, decision-making and social behavior, operating in informational, psychological, and cultural domains (NATO, 2021). Unlike traditional military operations, which rely on physical force or conventional information warfare, which focuses on disrupting communication systems, cognitive warfare targets the human mind directly. Its goal is to shape how individuals and communities interpret events, prioritize risks and make decisions.

Cognitive warfare can involve both state and non-state actors, ranging from governments seeking geopolitical advantage to ideological groups aiming to disrupt social cohesion. These actors leverage digital platforms, social media networks and other communication technologies to reach large populations efficiently. By tailoring narratives to specific cultural, social or demographic contexts, cognitive operations exploit existing societal divisions, psychological vulnerabilities and information gaps (Pomerantsev, 2019).

A critical feature of cognitive warfare is its dual objective: it simultaneously spreads targeted messages and undermines trust, creating confusion and destabilizing social cohesion. This combination weakens institutional legitimacy and erodes democratic processes, as public confidence in authorities, media and civil society becomes compromised (Rid, 2020). Unlike conventional threats, cognitive operations allow adversaries to influence societies without triggering overt retaliation.

Throughout history, cognitive strategies have existed in forms such as propaganda, psychological operations and ideological campaigns. What differentiates modern cognitive warfare is the scale, speed and precision enabled by digital connectivity. Artificial intelligence, algorithm-driven content distribution and micro-targeted advertising amplify messages across platforms, often bypassing traditional checks on accuracy.

Disinformation campaigns exploiting algorithmic amplification can reach millions within hours, shaping discourse and behavior before fact-checking or official responses can intervene (Bradshaw & Howard, 2019). For example, analysis of more than 14 million election-related tweets from the 2016

U.S. presidential campaign revealed that social bots were responsible for a disproportionate share of links to low-credibility sources, amplifying misinformation before fact-checking could intervene. These bots accounted for roughly 9–15% of all such links, demonstrating how algorithmic dynamics can rapidly propel false content through networks (Shao et al., 2018).

In practice, cognitive warfare operates across multiple layers:

- Individual level: influencing beliefs, attitudes and decision-making.
- Community level: exploiting social networks to amplify divisions and polarize discourse.
- Institutional level: undermining public trust, organizational credibility and policy effectiveness.

Thus, understanding cognitive warfare requires a multidisciplinary approach, integrating insights from psychology, communications, political science, cybersecurity and sociology. Its pervasive nature means that societies must treat it not just as a military or cybersecurity concern, but as a fundamental social challenge, impacting public trust, democratic legitimacy and societal resilience (Rid, 2020; NATO, 2021).

2.1 Differentiating cognitive warfare from other adjacent concepts

To prevent conceptual overreach and make the paper's argumentation more precise, it is essential to differentiate cognitive warfare from related terms. Table 1, presented below, aims to clarify such distinction and show that cognitive warfare is broader than disinformation, but narrower than hybrid warfare, with a unique focus on manipulating how societies process reality.

Table 1. Conceptual Distinctions between Cognitive Warfare and Adjacent Concepts

Concept	Definition	Distinction from cognitive warfare
Disinformation	Deliberately false or misleading information intended to deceive.	A tactic within cognitive warfare not the overarching strategy.
Propaganda	Systematic dissemination of information (biased or misleading) to promote a political cause or point of view.	Propaganda is mostly one-way interaction while cognitive warfare is interactive, adaptive and feedback driven.

Concept	Definition	Distinction from cognitive warfare
Information warfare	Manipulation of information and information systems through means like disruption of communication systems and data integrity.	It focuses on technical and infrastructure elements, not directly on human cognition.
Hybrid warfare	Combination of conventional and unconventional methods (military, cyber, economic)	Cognitive warfare is a component of hybrid warfare which targets the mind.
Psychological operations (PSYOPS)	Military-led activities to influence emotions and behavior.	They are typically state-driven and tactical. Cognitive warfare includes non-state actions and strategic societal manipulation.

(Based on author's analysis)

3. MECHANISMS OF COGNITIVE WARFARE

Cognitive warfare employs multiple methods simultaneously, combining information, technology and psychology to shape public perceptions.

3.1 Disinformation and narrative manipulation

Disinformation refers to deliberately false or misleading information designed to confuse, mislead or manipulate public perception (Wardle and Derakhshan, 2017). Unlike accidental misinformation, disinformation is intentional and often structured to exploit social vulnerabilities or pre-existing biases.

During the COVID-19 pandemic, disinformation campaigns circulated false claims regarding vaccine safety, virus origins and government health measures. Social media platforms and encrypted messaging apps amplified these narratives, contributing to public confusion and lower compliance with official guidance (World Health Organization [WHO], 2020).

In Europe, migration-related disinformation portrayed certain groups as existential threats, exacerbating societal tensions and fueling political polarization (European Commission, 2020).

Narrative manipulation often follows strategic framing: events are presented selectively to evoke emotional responses such as fear, outrage or moral indignation. By controlling the framing, cognitive actors can shift public opinion and normalize extreme positions over time (Pomerantsev, 2019).

3.2 Algorithmic amplification

Digital platforms rely on algorithms designed to maximize user engagement, often prioritizing sensational or polarizing content. Cognitive actors exploit this by crafting messages optimised for virality, effectively amplifying their impact without requiring mass coordination (Bradshaw and Howard, 2019). For instance, migration-related narratives in European countries were algorithmically amplified, exaggerating crime statistics or portraying minority groups as security threats. This process creates echo chambers, where individuals are repeatedly exposed to similar content, reinforcing existing biases and intensifying societal divisions (Allcott et al., 2020). Algorithmic amplification thus transforms disinformation campaigns into widespread social phenomena, influencing discourse and even political behavior.

3.3 Psychological targeting

Psychological targeting tailors messages to specific groups or individuals based on emotional, cultural and cognitive characteristics. This includes appeals to fear, identity, moral outrage or in-group loyalty, making narratives more persuasive and resistant to counter-messaging (Pomerantsev, 2019).

During conflicts in Eastern Europe, coordinated campaigns targeted both domestic and international populations with emotionally charged narratives that reinforced pre-existing social divisions. Such campaigns exploited uncertainty and fear to influence attitudes toward government policies, international organizations and foreign actors (Giles, 2016). By manipulating emotional responses, cognitive warfare can drive behavioral change, encourage self-censorship and shape public discourse without overt coercion.

3.4 Networked and coordinated Manipulation

Cognitive warfare increasingly relies on networked actors and automated tools. Bot networks, troll farms and coordinated inauthentic accounts amplify targeted messages, creating the illusion of grassroots support (astroturfing) or consensus. These coordinated campaigns can manipulate trending topics, distort public perception of popular opinion, and pressure policymakers to respond to perceived social demands (Bradshaw and Howard,

2019). For example, coordinated online campaigns during the Ukraine conflict spread narratives to both local and global audiences, combining emotionally charged imagery, selective facts and fabricated reports. The cumulative effect was not only confusion, but also diminished trust in news sources, humanitarian organizations and international institutions (Giles, 2016).

3.5 Integrated societal effects

The combination of disinformation, algorithmic amplification, psychological targeting and coordinated network activity generates pervasive cognitive shockwaves. Citizens struggle to identify reliable sources, social cohesion erodes and public discourse becomes highly polarised (Rid, 2020).

Moreover, these effects are self-reinforcing: exposure to manipulated content increases skepticism toward alternative viewpoints, making individuals more susceptible to subsequent campaigns. Over time, this creates an environment in which misinformation becomes normalised, trust in institutions diminishes and collective decision-making is impaired (Bradshaw and Howard, 2019).

By targeting multiple levels—individual, community and institutional—cognitive warfare produces structural societal impacts that extend beyond immediate events. The goal is not simply to disseminate false information, but to reshape the cognitive environment, influencing social norms, political participation and policy outcomes over the long term (Rid, 2020).

4. SOCIETAL IMPACT OF COGNITIVE WARFARE

Cognitive warfare affects more than individual perceptions; its effects ripple through society, reshaping behaviors, social norms and institutional trust (Rid, 2020). These impacts are structural, cumulative and multi-dimensional, influencing democratic governance, policy implementation and social cohesion.

4.1 Polarization and social fragmentation

One of the most visible effect is societal polarization. Disinformation campaigns often exploit pre-existing divisions—political, ethnic, religious or cultural—amplifying disagreements into entrenched societal fault lines (European Commission, 2020). This phenomenon is evident in several European countries, where migration-related disinformation exaggerated perceived threats posed by immigrant communities, prompting local populations to adopt more extreme positions. Such polarization hindered consensus-building on social and

policy matters, making cooperative decision-making more difficult and weakening democratic governance (Bradshaw and Howard, 2019).

Polarization also manifests in online environments. Social media platforms, by prioritizing engagement over accuracy, reinforce echo chambers, where individuals are repeatedly exposed to similar views and rarely encounter alternative perspectives (Allcott et al., 2020). The cumulative effect is a fragmented public discourse that erodes mutual understanding and trust between societal groups.

Research on migration discourse shows that social media and digital information environments have the power to amplify misleading narratives about migration and migrants, reinforcing biased interpretations and accelerating the spread of misinformation that influences public perception and fuels societal divisions (Komendantova et al., 2023). Evidence of this can be seen in the rapid diffusion of migration-related misinformation and fake news across social media platforms such as Facebook and X. Refugee-focused disinformation frequently identified by international fact-checking organizations among the most widely shared content, illustrating how algorithmic sharing dynamics can reinforce biased or misleading narratives before effective corrective responses occur (Olaru, 2023).

4.2 Erosion of public and institutional trust

Repeated exposure to conflicting, misleading or manipulated information undermines confidence in both authorities and institutions (Rid, 2020). At the public level, this manifests as declining trust in government, scientific bodies and mainstream media. During the COVID19 pandemic, widespread misinformation regarding vaccines, treatments and public health policies contributed to heightened skepticism among citizens. Countries with inconsistent communication or opaque decision-making experienced lower compliance with health measures and increased susceptibility to conspiracy theories (WHO, 2020).

Similarly, migration-related disinformation and other targeted campaigns have been shown to exaggerate perceived threats, prompting individuals to adopt more extreme positions and reinforcing societal divisions, thereby decreasing confidence in democratic processes and public institutions (Bradshaw and Howard, 2019). Such erosion of public trust impedes collective action and diminishes societal resilience in the face of crises.

Institutional trust is also affected, as manipulated narratives can diminish the credibility, legitimacy and operational capacity of organizations themselves. In political contexts, misinformation

surrounding elections, policy decisions or international agreements reduces confidence in democratic institutions, impairing their effectiveness (OECD, 2021).

Likewise, during the Ukraine conflict, coordinated online campaigns targeted humanitarian organizations and official reporting channels, generating doubt about operational integrity and impartiality. The resulting mistrust complicated both domestic and international responses, illustrating how cognitive warfare can produce lasting societal and operational consequences (Giles, 2016).

Together, these examples demonstrate that misinformation and cognitive warfare do not only affect individual perceptions, but also compromise institutional resilience, creating a feedback loop where declining public trust further undermines the credibility and effectiveness of key organizations. Addressing these challenges requires strengthening both societal awareness and institutional transparency to preserve democratic governance and societal cohesion.

4.3 Behavioral shifts and risk aversion

Cognitive warfare campaigns also influence individual and collective behaviors. Fear-based narratives and emotionally charged content can make populations more risk-averse, less willing to engage in public life, or more prone to adopting self-protective behaviors based on misinformation (Pomerantsev, 2019).

This is evident in online campaigns exaggerating crime or security threats associated with migration, which led some communities to reduce social engagement and participation in local governance. Political mobilization can also be affected, as manipulated narratives discourage voting or create overreliance on partisan information channels (Bradshaw and Howard, 2019).

These behavioral shifts reinforce societal divisions, creating feedback loops that amplify the effectiveness of cognitive warfare campaigns and extend their impact over time (Rid, 2020).

5. DEMOCRATIC CHALLENGES AND POLICY DILEMMAS

Cognitive warfare presents long-term, structural challenges to democratic societies. Beyond immediate disinformation or manipulated narratives, persistent exposure erodes trust in institutions, deepens social polarization and normalizes misinformation, ultimately weakening collective decision-making and civic engagement (Rid, 2020; OECD, 2021). Citizens may become less willing to collaborate, less trusting

of authorities and more vulnerable to future manipulation.

Democracies face a unique dilemma in responding to these threats. Constitutional protections—such as freedom of expression, privacy and open debate—limit the tools governments can use to counter manipulation (Nissenbaum, 2010). Policymakers must balance the risk of underreaction, which allows cognitive attacks to spread and amplify societal divisions, with the risk of overreaction, potentially infringing civil liberties, provoking public backlash and further eroding trust (Wardle and Derakhshan, 2017; Rid, 2020).

The complexity of digital platforms adds to the challenge. Algorithm-driven, decentralized networks facilitate the rapid spread of both factual and manipulative content, while asymmetric adversaries exploit these systems with bots, deepfakes, and targeted campaigns, often acting faster than democracies can respond (Bradshaw and Howard, 2019; European Commission, 2020; Nissenbaum, 2010).

Effectively addressing these challenges requires a multi-level approach that integrates societal awareness, institutional transparency and legally grounded policy interventions. Strengthening media literacy, fostering public engagement and maintaining adaptive, accountable governance are essential to preserve democratic norms while mitigating the long-term impacts of cognitive warfare (Guess, Nagler and Tucker, 2020; OECD, 2021).

5.1 Digital complexity and rapid evolution

Digital platforms amplify the complexity of democratic responses. Social media ecosystems are global, decentralised and algorithmically driven, enabling rapid dissemination of both factual and manipulative content (Bradshaw and Howard, 2019).

Policymakers struggle to monitor and mitigate disinformation without unintentionally affecting legitimate speech. This challenge became apparent during attempts to regulate online content amid migration crises, where measures intended to suppress harmful narratives were sometimes criticised as politically biased, demonstrating the difficulty of regulating information in a manner perceived as neutral and fair (European Commission, 2020).

Cognitive threats are often deployed by actors with minimal accountability, who exploit the openness of democratic societies. Such adversaries can use sophisticated tactics—bot networks, deepfakes and targeted micro-advertising—to manipulate specific populations without leaving clear evidence of coordination (Bradshaw and Howard, 2019).

Democratic institutions, in contrast, are constrained by checks, debates and procedural safeguards. This asymmetry creates a persistent

vulnerability: adversaries can act quickly, while democracies respond slowly and cautiously to avoid overstepping legal or ethical boundaries (Nissenbaum, 2010).

5.2 Societal participation and normative considerations

As is widely understood today, citizens in democracies are not passive recipients of information—they are active participants in public discourse. Responses to cognitive threats therefore cannot rely solely on top-down enforcement; they require societal engagement, education and trust-building (Guess, Nagler and Tucker, 2020).

Policymakers must integrate normative considerations into strategy: defending against manipulation without compromising democratic freedoms. This involves fostering critical thinking, promoting media literacy and reinforcing public trust in institutions, while carefully calibrating legal and regulatory interventions (OECD, 2021).

5.3 Multi-Level strategic response

The central challenge is both practical and ethical: how to preserve democratic norms while mitigating cognitive threats. Effective responses require:

- Multi-level coordination across government, civil society and media sectors.
- Transparent and accountable institutional practices.
- Education and empowerment of citizens to critically assess information.
- Technological solutions, including platform-level monitoring, that respect privacy and freedom of expression.

Ultimately, democratic resilience depends on the ability to integrate societal, institutional and legal strategies. Only by harmonizing protection, education and transparency can democracies counter cognitive warfare without undermining the very freedoms that define them (Rid, 2020; Nissenbaum, 2010).

6. STRENGTHENING SOCIETAL RESILIENCE

Societal resilience—the capacity of communities and institutions to anticipate, absorb, adapt to and recover from cognitive shocks—is central to countering contemporary information threats (Rid, 2020). Unlike traditional military risks, cognitive warfare exploits social vulnerabilities, requiring resilience to operate simultaneously at individual, institutional and systemic levels. Effective responses must therefore be proactive, enabling both citizens and institutions to recognize, resist and adapt to manipulation within increasingly complex information environments.

At the individual level, media literacy and critical thinking play a foundational role in reducing

susceptibility to disinformation. Education initiatives that strengthen citizens' ability to evaluate sources, detect bias and verify information contribute directly to informed civic participation and limit the societal reach of manipulative narratives (Guess, Nagler and Tucker, 2020).

At the institutional level, transparency, accountability and consistent communication reinforce public trust, which acts as a critical buffer against cognitive manipulation. Evidence from recent crises, including the COVID-19 pandemic, suggests that open and credible communication significantly reduces the impact of misleading narratives on public behavior (OECD, 2021; WHO, 2020).

At the systemic level, resilience depends on adaptive governance and cross-sector collaboration. Partnerships between governments, civil society, media organizations and technology platforms enable the timely detection and mitigation of disinformation, improving responsiveness in rapidly evolving digital environments (Bradshaw and Howard, 2019; European Commission, 2020).

At the same time, long-term resilience is supported by cultural and normative foundations that promote critical inquiry, trust and active civic engagement.

Ultimately, societal resilience is maximised when these dimensions are integrated into a coherent framework. The interaction between informed citizens, trustworthy institutions and adaptive governance structures strengthens social cohesion and democratic stability, enabling societies to absorb cognitive shocks without resorting to restrictive measures that could undermine fundamental rights (Nissenbaum, 2010).

To synthesise the analysis above, the main findings can be summarised as follows:

Table 2. Summary of cognitive warfare elements

Mechanism	Primary target	Societal effect	Policy response
Disinformation and narrative manipulation	Individual beliefs	Polarization, confusion	Media literacy, fact checking
Algorithmic amplification	Community discourse	Echo chamber, fragmentation	Platform regulation, transparency
Psychological targeting	Emotional/cognitive vulnerabilities	Risk aversion, behavioural shifts	Public awareness campaigns

Mechanism	Primary target	Societal effect	Policy response
Network coordination (bots, trolls)	Institutional trust	Erosion of credibility, legitimacy	Cross sector monitoring, legal frameworks
Integrated cognitive shockwaves	Entire society	Weakened democratic participation	Adaptive governance, civic engagement

(*Based on the author's analysis*)

7. RECOMMENDATIONS

Building on the dimensions of societal resilience outlined in the previous section, policy responses to cognitive warfare require the translation of these principles into coordinated policy and societal actions. Resilience must be operationalised across individual, institutional and systemic levels in order to address the multifaceted nature of cognitive threats.

At the individual level, media literacy and critical thinking should be integrated into formal education and complemented by public awareness initiatives, thus enabling citizens to navigate complex information environments.

At the institutional level, transparency, accountability and consistent public communication are critical in maintaining trust and limiting the impact of disinformation. Therefore, public authorities should adopt these principles and establish dedicated structures or rapid response mechanisms for identifying and countering manipulation campaigns thus enhancing institutional resilience.

At the systemic level, adaptive governance and cross-sector collaboration between governments, civil society, media and technology platforms enable the timely detection and mitigation of coordinated manipulation campaigns. Supporting independent fact-checking mechanisms further enhances information credibility and reinforces public confidence in verified sources. Policy makers should promote regulatory frameworks for digital platforms that are necessary to address algorithmic amplification and coordinated disinformation, while safeguarding freedom of expression and democratic norms.

Integrating these measures into a coherent and adaptive strategy ensures that societal resilience is not only reactive, but also preventive. By aligning education, institutional integrity and governance mechanisms, societies can effectively mitigate cognitive threats while preserving trust, social cohesion and democratic values.

8. CONCLUSIONS

Cognitive warfare represents a structural and evolving challenge to contemporary democratic societies, operating through indirect, cumulative mechanisms that target perception, trust and social cohesion. As demonstrated throughout this article, its impact extends beyond the dissemination of disinformation, affecting behavioral patterns, institutional legitimacy and the quality of public discourse. As a conceptual review, this article does not claim to present original empirical findings, but rather synthesises existing evidence to identify patterns and implications.

Unlike traditional forms of conflict, cognitive warfare exploits the openness of democratic systems, creating a persistent tension between safeguarding security and preserving fundamental freedoms. The findings highlight that vulnerability does not stem solely from technological exposure, but from underlying societal factors such as polarization, declining trust and limited critical media engagement.

In this context, societal resilience emerges as a central pillar in mitigating cognitive threats. However, resilience cannot be understood as a purely defensive capacity rather, it reflects the ability of societies to adapt, learn and maintain democratic integrity under conditions of informational pressure. Strengthening this resilience requires coordinated efforts across individual, institutional and systemic levels, ensuring that responses remain consistent with democratic norms and values.

Ultimately, the challenge of cognitive warfare is not only to counter manipulation, but also to strengthen the underlying cognitive and normative conditions that sustain democratic systems.

REFERENCES

[1] Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). *The welfare effects of social media*. *American Economic Review, 110*(3), 629676. https://doi.org/10.1257/aer.20190658

[2] Allen, J., Howland, B., Möbius, M., Rothschild, D., & Watts, D. J. (2020). *Evaluating the fake news problem at the scale of the information ecosystem*. Science Advances, 6(14), eaay3539. https://www.science.org/doi/10.1126/sciadv.aay3539

[3] Bennett, W. L., & Livingston, S. (2018). *The disinformation order: Disruptive communication and the decline of democratic institutions*. European Journal of Communication, 33(2), 122–139. https://doi.org/10.1177/0267323118760317

[4] Bjola, C., & Holmes, M. (2015). *Digital diplomacy: Theory and*

practice. Routledge.

[5] *Cyber influence and international security*. (2009). In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (pp. 343–361). Potomac Books.

[6] European Commission. (2020). *Joint communication on tackling COVID-19 disinformation: Getting the facts right*. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0008

[7] European Commission. (2020). *A strengthened EU Code of Practice on Disinformation* https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en

[8] Giles, K. (2016*). Handbook of Russian information warfare: Challenging the skeptics*. NATO Strategic Communications Centre of Excellence. https://www.ndc.nato.int/download/handbook-of-russian-information-warfare-by-keir-giles/

[9] Guess, A., Nagler, J., & Tucker, J. (2020). *Less than you think: Prevalence and predictors of fake news dissemination on Facebook*. Science Advances, 6(7), eaay3539. https://pubmed.ncbi.nlm.nih.gov/30662946/

[10] Howard, P. N., & Bradshaw, S. (2018). *The global organization of social media disinformation campaigns*. Journal of International Affairs, 71(1.5)

[11] NATO Innovation Hub. (2021). Cognitive warfare. NATO. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

[12] Komendantova, N., Erokhin, D., & Albano, T. (2023). *Misinformation and its impact on contested policy issues: The example of migration discourses*. Societies, 13(7), 168. https://doi.org/10.3390/soc13070168

[13] Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[14] Olaru, G. O. (2023). *The rapid diffusion of fake news: An analysis of content on migration, refugees, and conflict on international factchecking platforms*. *Connectist: Istanbul University Journal of Communication Sciences, Issue 65*, 61–87. https://doi.org/10.26650/CONNECTIST2023-1404666

[15] OECD. (2021). *Trust and public policy: How better governance can help rebuild public trust*. OECD Publishing. https://www.oecd.org/en/publications/trust-and-public-policy_9789264268920-en.html

[16] Pomerantsev, P. (2020). *This is not propaganda: Adventures in the war against reality*. Faber & Faber.

[17] Rid, T. (2020). *Active measures: The secret history of disinformation*

and political warfare. Farrar, Straus and Giroux.

[18] Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). *The spread of low-credibility content by social bots. Nature Communications*, 9, 4787. https://doi.org/10.1038/s41467-018-06930-7

[19] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making (Council of Europe Report DGI(2017)09)*. Council of Europe. https://www.firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-de%CC%81sinformation-1.pdf

[20] World Health Organization, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, & IFRC. (2020, September 23). Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. World Health Organization. https://www.who.int/news/item/23-09-2020-managing- the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation