

Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Cezar Vasilescu, *Connections QJ* 24, no. 3 (2025): 51-76
https://doi.org/10.11610/Connections.24.3.03

Research Article

Cognitive Warfare and Societal Resilience: Between Doctrinal Claims and Empirical Evidence

Cezar Vasilescu

Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, Romania, https://www.dresmara.ro

Abstract: This article examines cognitive warfare within the conceptual framework developed by NATO Allied Command Transformation, which treats the cognitive domain as a distinct and increasingly central dimension of modern conflict. It also draws on the Russian and Chinese strategic traditions, which have a longer intellectual lineage (reflexive control and the "Three Warfares" doctrine, respectively). Cognitive warfare uses psychological manipulation, disinformation, and emerging technologies to influence perceptions, undermine societal cohesion, and erode institutional trust, operating primarily through informational and psychological means rather than kinetic force. Based on a critical review of academic literature, policy documents, and case studies, the article traces how state and non-state actors have developed cognitive warfare tactics and assesses their implications for national security and democratic resilience. A comparative analysis of national responses identifies key vulnerabilities and countermeasures, with particular attention to how AI-driven influence operations and big data analytics have reshaped both offensive strategies and defensive resilience measures. The article concludes with policy recommendations that emphasize adaptive strategies to safeguard information integrity and democratic stability against evolving hybrid threats.

Keywords: cognitive warfare, societal resilience, disinformation, hybrid threats, artificial intelligence, influence operations, information security.

Introduction

Within the NATO Allied Command Transformation conceptual tradition adopted here, cognitive warfare (CW) has been framed as a defining element of contemporary conflict, understood to shape perceptions, influence behavior, and target

Creative Commons BY-SA 4.0

societal cohesion.[1] Whether the observable effects of cognitive-warfare tactics on public attitudes and behavior match this doctrinal framing is a separate empirical question, and one this article addresses directly. Unlike conventional military confrontations, cognitive warfare is said to operate within the human mind, targeting belief systems, decision-making processes, and trust in institutions. Digital communication infrastructures and artificial intelligence have expanded the scale at which state and non-state actors can attempt to shape narratives. The *3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats* documents 505 FIMI incidents in 2024, involving approximately 38,000 channels and targeting 322 organizations across 90 countries.[2] Whether these attempts produce durable changes in public attitudes and behavior is a different matter, and the empirical literature answers it with far more caution than doctrinal framings imply.[3] This article traces the evolution of cognitive warfare, examines its key mechanisms and its implications for democratic societies, and considers strategies for strengthening resilience against the threats attributed to it.

Understanding the mechanisms and empirical effects of cognitive warfare requires situating it within broader historical and geopolitical contexts. Psychological operations and propaganda have long been instruments of government. The contemporary information environment, characterized by algorithm-driven social media platforms, AI-enhanced influence campaigns, and the weaponization of big data, has increased the complexity of cognitive threats. The erosion of public trust in institutions, the polarization of societies, and the manipulation of collective memory have long been deliberate objectives of psychological warfare and propaganda. What has changed is the industrial scale, the personalization, and the doctrinal institutionalization of the operations directed at these objectives.

Research Objectives and Key Questions

This study analyzes the mechanisms of cognitive warfare and assesses strategies for strengthening societal resilience. It aims to examine the evolution of cognitive warfare and its role in modern conflicts; identify key tactics used in cognitive

---

1 NATO Allied Command Transformation (ACT), "Cognitive Warfare," accessed July 29, 2025, https://www.act.nato.int/activities/cognitive-warfare.

2 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (Brussels: EEAS, March 2025), 9, https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

3 Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences* 117, no. 1 (2020): 243–250, 243, https://doi.org/10.1073/pnas.1906420116; Sacha Altay, Manon Berriche, and Alberto Acerbi, "Misinformation on Misinformation: Conceptual and Methodological Challenges," *Social Media + Society* 9, no. 1 (2023): 1, https://doi.org/10.1177/20563051221150412.

operations, particularly in the digital era; and evaluate strategies for strengthening societal resilience against them.

To achieve these objectives, the study is guided by the following key research questions:

1. What are the primary methods and tactics employed in cognitive warfare today?
2. How do cognitive operations impact public trust, decision-making, and societal cohesion?
3. Which strategies strengthen societal resilience against cognitive operations?

Research Methodology

This article adopts a qualitative methodology, incorporating a multidisciplinary approach that draws on security studies, cognitive psychology, media analysis, and military strategy. The research is based on a critical review of academic literature, policy reports, and case studies that illustrate the use of cognitive warfare tactics in contemporary conflicts.

The theoretical lens used here warrants explicit statement. The cognitive-psychology framework relies on the dual-process account of cognition (System 1 heuristic processing; System 2 analytical processing), the heuristics-and-biases tradition after Kahneman and Tversky, and motivated-reasoning models.

This framework has known limitations. The strong distinction between automatic and controlled processing is contested in current cognitive science, which increasingly favors embodied and predictive-processing accounts. The framework is also fundamentally individual-level: applying it to societal-level phenomena requires additional assumptions, and different theoretical lenses (social identity theory; Durkheim's sociology of cohesion [4] and Weber's of legitimacy [5]) can produce different accounts of the same empirical patterns. This article uses cognitive psychology as one input alongside sociological and science-and-technology-studies perspectives, and flags interpretive dependence on the framework where it arises.

A comparative case study approach is employed to examine how different societies have responded to cognitive threats, highlighting both vulnerabilities and effective countermeasures. Primary sources include government reports, intelligence assessments, and official statements from NATO and EU institutions on disinformation and cognitive security. Secondary sources consist of peer-reviewed journal articles and expert analyses from think tanks specializing in hybrid warfare and strategic resilience.

---

[4] Émile Durkheim, *The Division of Labor in Society*, trans. George Simpson (New York: Macmillan, 1933), 111.

[5] Max Weber, *Economy and Society: An Outline of Interpretive Sociology*, ed. Guenther Roth and Claus Wittich, trans. Ephraim Fischoff et al. (Berkeley: University of California Press, 1978), 212-16.

The article is organized around one central argument, presented here in explicit independent-variable, causal-logic, and dependent-variable form to make the analytical structure transparent:

- *Independent variable*: cognitive-warfare tactics as cataloged in the Tactics section below;
- *Causal logic*: exposure amplification through algorithmic curation, engagement optimization through affective content, and network infiltration through inauthentic accounts and coordinated behavior;
- *Dependent variables*: societal cohesion, institutional trust, and societal resilience.

The article argues that, based on current empirical evidence, the observable effect of cognitive-warfare tactics on the dependent variables is primarily to reinforce pre-existing attitudes and exploit pre-existing societal cleavages, rather than produce durable belief change ex nihilo. If correct, this finding has direct implications for what resilience strategies can plausibly achieve, as developed in the National Responses section below.

Conceptualizing the Core Terms: Social Cohesion, Trust, Legitimacy, and Societal Resilience

The core terms of this analysis (social cohesion, institutional trust, institutional legitimacy, and societal resilience) carry a heavier conceptual load than the cognitive-warfare literature typically acknowledges. Each has an established meaning in sociology, political theory, and policy, and each of those meanings shapes the claims that can plausibly be made about the societal-level effects of cognitive operations. The paragraphs that follow set out these meanings before the argument proceeds.

Social cohesion is understood here in the tradition running from Durkheim's account of organic solidarity to the Bertelsmann Stiftung's Social Cohesion Radar.[6] It denotes the quality of social relations characterized by durable networks, acceptance of diversity, and a shared orientation toward the common good. It emerges from repeated social interactions and cannot be produced by decree. Where cognitive operations are directed at cohesion, the mechanism is not the creation of new social divisions but the amplification and instrumentalization of pre-existing ones.

Institutional trust is understood here as an achieved relational quality between citizens and institutions, generated through interactions in which institutions behave in ways that are intelligible, competent, and consistent with their

[6] Georgi Dragolov et al., *Social Cohesion Radar – Measuring Common Ground: An International Comparison of Social Cohesion, Methods Report* (Gütersloh: Bertelsmann Stiftung, 2013), 5, https://aei.pitt.edu/74134/1/Social_cohesion_radar.pdf.

stated purposes. In this respect, Levi [7] and Rothstein and Teorell [8] provide the operative political-science explanations.

Institutional legitimacy, in turn, is the socially recognized right of an institution to make mandatory decisions, which Weber grounds in tradition, charisma, or legal-rational procedure. Neither trust nor legitimacy can be "imposed"; both are relational outcomes.

Societal resilience is used here in the broader sociological and policy sense articulated by Bourbeau,[9] Chandler,[10] and the *2025 Strategic Foresight Report* ("Resilience 2.0"),[11] rather than in the narrow infrastructural or cybersecurity sense often used in doctrinal writing. It denotes a society's capacity to absorb shocks, adapt institutions, and preserve democratic functioning under stress. It is a distributed property of institutions, civic infrastructure, and interpersonal networks, not a property of individuals. Where an individual-level concept is genuinely required in the argument that follows, epistemic autonomy [12] is used, defined as the capacity of the individual to question assumptions and resist misleading information under uncertainty.

As noted in the Methodology section, individual-level cognitive-psychology mechanisms do not automatically aggregate to societal-level outcomes. This article attributes societal-level effects to the sociological mechanisms discussed above, rather than treating these effects as the numerical sum of individual biases.

Critical Review of Academic Literature and Policy Documents

Within the NATO/EU/US tradition adopted here, cognitive warfare has become institutionalized as a distinct operational domain over the past two decades. This does not mean that kinetic warfare has been replaced; the intensity of kinetic operations in Ukraine since 2022, in Gaza since 2023, and elsewhere makes it

---

7 Margaret Levi, "A State of Trust," in *Trust and Governance*, ed. Valerie A. Braithwaite and Margaret Levi (New York: Russell Sage Foundation, 1998), 85-87.

8 Bo Rothstein and Jan Teorell, "What Is Quality of Government? A Theory of Impartial Government Institutions," *Governance: An International Journal of Policy, Administration, and Institutions* 21, no. 2 (2008): 165–190, 170, https://doi.org/10.1111/j.1468-0491.2008.00391.x.

9 Philippe Bourbeau, "Resiliencism: Premises and Promises in Securitisation Research," *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013): 3–17, 3–5, https://doi.org/10.1080/21693293.2013.765738.

10 David Chandler, *Resilience: The Governance of Complexity* (Abingdon: Routledge, 2014), 2-3.

11 European Commission, *2025 Strategic Foresight Report – Resilience 2.0: Empowering the EU to Thrive Amid Turbulence and Uncertainty*, COM(2025) 484 final (Brussels: European Commission, September 9, 2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0484.

12 Jonathan Matheson, "The Philosophy of Epistemic Autonomy: Introduction to Special Issue," *Social Epistemology* 38, no. 3 (2024): 267–273, 267–268, https://doi.org/10.1080/02691728.2024.2335623.

plain that cognitive and kinetic operations run in parallel rather than in sequence. What has changed is that cognitive operations have been formalized as a coordinated operational domain alongside land, sea, air, cyber, and space, and integrated with kinetic operations within an overarching hybrid strategy.

Once confined largely to the realm of psychological operations and propaganda, cognitive warfare has emerged as a multidimensional and persistent strategy employed by both state and non-state actors, enabled by digital technology, social media ecosystems, and advances in neuroscience and behavioral science. The transition is not only terminological. It reflects a paradigm shift in which the human mind is reframed as the primary battlespace, targeted not only to alter opinions but also to reshape the very architecture of cognition (including decision-making, emotional regulation, and memory encoding), with the aim of shaping societal behavior and political outcomes. Nevertheless, whether external actors in fact achieve durable influence at this level remains empirically contested: a large study of Russian Internet Research Agency accounts, for example, found no evidence of substantial effects on the political attitudes and behaviors of American Twitter users.[13]

Early conceptualizations, such as Libicki's pioneering work on information warfare,[14] recognized the expanding battlefield of influence, yet they did not fully anticipate a cognitive domain that is conceptually distinct from kinetic warfare. While information warfare targets the content of the narrative, doctrinal writings on cognitive warfare frame the practice as targeting the interpretive processes through which that narrative is received [15] – a distinction that is analytically useful but should not be read as an empirical claim about achieved effect. In doctrinal terms, it is a strategy that seeks to manipulate the underlying interpretive frameworks through which individuals perceive reality, often bypassing rational cognition and exploiting subconscious biases. NATO's recent doctrinal developments have clarified this evolution by defining cognitive warfare as the "weaponization of public opinion," [16] thereby emphasizing its psychological, behavioral, and sociopolitical dimensions. This definition underscores the

[13] Robin Burda, *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds* (The Hague: The Hague Centre for Strategic Studies, June 2023), 3, https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf; Bail et al., "Assessing Russian Internet Research Agency's Impact," 246.

[14] Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995), 35-48, 95-96, https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf.

[15] Bernard Claverie and François du Cluzel, "The Cognitive Warfare Concept," NATO Allied Command Transformation Innovation Hub, 2022, 3, https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

[16] NATO ACT, "Cognitive Warfare."

shift from episodic propaganda to integrated influence operations that are described as synthesizing artificial intelligence, behavioral economics, and neurobiological insights to orchestrate systemic manipulation.[17]

This strategic innovation corresponds with a broader hybridization of conflict, in which cognitive warfare increasingly intersects with gray-zone tactics and hybrid operations, particularly in the doctrines of geopolitical rivals such as Russia and China. These actors have refined cognitive operations into a cornerstone of their strategic posture, deploying them to subtly fracture the internal cohesion of democratic adversaries without crossing the thresholds of traditional warfare.[18]

Societal resilience, as previously defined, denotes the capacity to absorb shocks, adapt institutions, and preserve democratic functioning under stress, rather than referring narrowly to infrastructure or cybersecurity. The empirical picture is more nuanced. Systematic evidence on digital-media use and democracy shows associations with declining political trust and increased polarization in established democracies, and with increased political participation and information consumption in autocracies and emerging democracies.[19] These are aggregate effects of digital media, not of external influence operations specifically. The narrower question of whether documented external influence operations produce measurable attitude change has been tested directly in at least one large study. Bail and coauthors [20] found no evidence that interaction with Russian Internet Research Agency accounts substantially affected six distinct measures of political attitudes and behavior among a longitudinal sample of American Twitter users. Altay, Berriche, and Acerbi synthesize the broader measurement critique into six misconceptions that inflate estimates of misinformation prevalence and impact.[21] Where cognitive operations do show observable effects, the effect is typically one of reinforcing existing predispositions and

[17] François du Cluzel, "Cognitive Warfare, a Battle for the Brain," keynote 3 in Mitigating and Responding to Cognitive Warfare, STO-MP-HFM-334 (Paris: NATO Science and Technology Organization, 2022), KN3-3, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf.

[18] Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," *Journal of Global Security Studies* 7, no. 4 (2022): ogac016, 1-2, https://doi.org/10.1093/jogss/ogac016; Christoph Deppe and Gary S. Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept," *Frontiers in Big Data* 7 (2024): 1452129, 2, https://doi.org/10.3389/fdata.2024.1452129.

[19] Philipp Lorenz-Spreen, Lisa Oswald, Stephan Lewandowsky, and Ralph Hertwig, "A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy," *Nature Human Behaviour* 7, no. 1 (2023): 74, https://doi.org/10.1038/s41562-022-01460-1.

[20] Bail et al., "Assessing Russian Internet Research Agency's Impact," 243.

[21] Altay, Berriche, and Acerbi, "Misinformation on Misinformation," 2.

exploiting preexisting cleavages rather than creating new beliefs.[22] These operations are not random; they systematically exploit confirmation bias, identity-based narratives, and emotional heuristics, leveraging digital platforms to inflame ideological cleavages and, in their intended effect, to paralyze decision-making processes.[23] In this environment, societal resilience becomes a function of digital literacy, institutional adaptability, and the cultivation of narrative competence, defined here as a population's ability to critically engage with and resist manipulative discourse.

The Effects Question: What the Evidence Does and Does Not Show

The measurement literature on the effects of external influence operations diverges sharply from the doctrinal literature, which assumes that those effects are large and durable. One study and one review anchor the point. Bail and co-authors merged non-public Twitter data on the Russian Internet Research Agency (IRA) with longitudinal survey data on 1,239 Republican and Democratic Twitter users from late 2017. Using Bayesian regression tree models, they found no evidence that interaction with IRA accounts substantially affected six distinct measures of political attitudes and behavior over the period studied. The users who interacted most with IRA accounts were those with strong ideological homophily within their existing networks, high interest in politics, and high frequency of Twitter use – the users least likely to be moved by any specific intervention.[24]

The broader measurement critique outlines six misconceptions that inflate estimates of misinformation prevalence and impact.[25] Among them are:

- engagement metrics are not measures of belief;
- sharing is not endorsement;
- people consume misinformation largely to socialize, express skepticism, or signal group membership; and
- acceptance of misinformation is heavily conditioned by prior predispositions.

These findings do not imply that cognitive operations are harmless. They imply that the causal chain from operation to attitude change is longer, more conditional, and more dependent on the characteristics of the receiving society than the doctrinal framing suggests.

---

[22] Lorenz-Spreen et al., "A Systematic Review of Worldwide Causal and Correlational Evidence," 76-78.

[23] Kathy Cao et al., "Countering Cognitive Warfare: Awareness and Resilience," NATO Review, May 20, 2021, accessed May 14, 2025, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

[24] Bail et al., "Assessing Russian Internet Research Agency's Impact," 244-245.

[25] Altay, Berriche, and Acerbi, "Misinformation on Misinformation: Conceptual and Methodological Challenges," 2.

A single case usefully illustrates the point. The 2016 Lisa F. case in Germany—a fabricated story of a 13-year-old Russian-German girl allegedly kidnapped and raped by migrants, amplified by Russian state media and Russian consular statements—provoked short-term protests in the Russian-German community and a diplomatic incident. It did not, however, shift underlying attitudes toward migration policy or Germany's political trajectory. Where the operation produced observable effects, those effects turned on an existing cleavage over migration and Russian-German identity; where it tried to produce new beliefs, it appears to have failed. This pattern—visible, short-run, cleavage-exploiting effects that do not aggregate into durable political change—is consistent across the empirical literature.

One further distinction matters for the remainder of the argument: the aggregate effect of digital media on democracy (studied by Lorenz-Spreen and coworkers [26] and others) is a different empirical question from the effect of specific external influence operations (studied by Bail and colleagues and Altay, Berriche, and Acerbi).[27] Conflating the two—attributing to specific influence operations the aggregate effects of digital-media use—is a logical leap that produces overstated threat assessments and inefficient policy responses.

The implications are particularly stark for democratic societies, where trust, cohesion, and legitimacy are not imposed but generated in social interactions: legitimacy as an achieved relational quality in Weber's sense, cohesion as an emergent property of collective conscience and organic solidarity in Durkheim's sense, and trust as a relational institutional outcome.[28] The infiltration of cognitive space with manipulative narratives undermines the epistemic conditions necessary for democratic consensus, replacing dialogue with suspicion and critical thought with ideological entrenchment.[29] Consequently, technocratic approaches to resilience—the enforcement architecture of the EU Digital Services Act, the NATO cognitive-warfare technical-tool program, algorithmic detection systems—are therefore necessary but not sufficient. They must be combined with civic education, pluralistic media, and inclusive discourse, which together reinforce society's ability to discern, deliberate, and decide under conditions of uncertainty and pressure.

---

[26] Lorenz-Spreen et al., "A Systematic Review of Worldwide Causal and Correlational Evidence."

[27] Bail et al., "Assessing Russian Internet Research Agency's Impact"; Altay, Berriche, and Acerbi, "Misinformation on Misinformation: Conceptual and Methodological Challenges."

[28] Levi, "A State of Trust," 85-87; Bo Rothstein, *The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective* (Chicago: University of Chicago Press, 2011), chaps. 1–2.

[29] Robert Reczkowski and Andrzej Lis, "Cognitive Warfare: What Is Our Actual Knowledge and How to Build State Resilience?" *Bezpieczeństwo. Teoria i Praktyka (Security Theory and Practice)* 48, no. 3 (2022): 51–61, 57, https://doi.org/10.48269/2451-0718-btip-2022-3-003.

As Nikoula and McMahon underscore,[30] the battlefield has moved inward: rather than targeting infrastructure or military assets, adversaries now aim to compromise a society's cognitive coherence. The long-run erosion of institutional trust in liberal democracies has domestic drivers—economic dislocation, elite failures, media commercialization, and partisan sorting—that predate and do not depend on external influence operations.[31,32] External cognitive operations may exploit or amplify this erosion, but they are not its cause. Reversing the underlying erosion therefore requires domestic institutional and political interventions, not merely kinetic or cyber deterrence directed at external actors. It also demands a cultural and epistemological counter-strategy that empowers citizens as active agents of their own cognitive security.

The Gap Between Doctrinal Maturity and Empirical Uncertainty

The literature reviewed above supports the following characterization of the current state of knowledge and identifies the gap this article addresses. First, the doctrinal literature on cognitive warfare, produced by NATO Allied Command Transformation, the NATO Innovation Hub, and adjacent policy institutions, has matured rapidly and now presents cognitive warfare as a distinct operational domain with a stable taxonomy of tactics. Second, the empirical literature on the effects of those tactics on public attitudes and behavior is thin and contested; the most methodologically careful studies point toward smaller and more conditional effects than doctrine implies. Third, the concepts that underpin the understanding of cohesion, trust, and resilience are typically undertheorised in cognitive-warfare writing, even though they are well developed in sociology and political science.

The gap this article addresses lies between the first and second characterizations. The article takes doctrinal maturity seriously as an object of analysis, applies the sociological concepts rigorously, and enforces the empirical distinction that the effects literature demands. The result is a critical taxonomy that specifies what cognitive-warfare tactics aim to achieve, distinguishes this from what they measurably achieve, and grounds resilience recommendations in the empirical picture rather than in the doctrinal one.

In conclusion, cognitive competition has long been an aspect of strategic competition and predates the current NATO doctrinal vocabulary. What has changed over the past two decades within the NATO/EU/US tradition is the industrialization, personalization, and doctrinal institutionalization of cognitive operations, not the existence of a cognitive dimension to strategic competition.

---

[30] Daniel Nikoula and Dave McMahon, "Cognitive Warfare: Securing Hearts and Minds" (Ottawa: University of Ottawa, July 2024), 3, https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf.

[31] Pippa Norris, *Democratic Deficit: Critical Citizens Revisited* (New York: Cambridge University Press, 2011), 8.

[32] Levi, "A State of Trust," 85-87.

This framing carries a normative implication that should be admitted openly: labeling a long-standing practice a new form of "warfare" creates policy demands that would not follow from describing it in more neutral terms. No longer limited to episodic campaigns of influence or disinformation, cognitive warfare now operates as a persistent, multidimensional threat that can undermine the foundational mechanisms through which societies construct meaning, exercise judgment, and maintain cohesion.[33,34] If that assessment holds, safeguarding democratic resilience requires societies to broaden their conception of security beyond protecting borders or networks to fortifying minds through education, civic empowerment, and a reinvigorated commitment to epistemic integrity.

Tactics and Implications for Security and Democratic Resilience

The modern conceptualization of cognitive warfare builds on the historical foundation of psychological operations but has been significantly transformed and intensified by the proliferation of digital technologies. These technologies enable state and non-state actors to engage in complex influence operations that exploit human cognition through misinformation, deepfakes, and algorithmically curated narratives designed to erode societal cohesion and democratic resilience.[35] Unlike conventional warfare, which relies on territorial occupation or kinetic superiority, cognitive warfare is inherently asymmetrical and non-linear, seeking to exploit the vulnerabilities of open societies by targeting belief systems, trust networks, and public discourse. At its core, cognitive warfare leverages cognitive biases (such as confirmation bias and the illusory truth effect) to subtly influence perceptions, making individuals more likely to accept repeated falsehoods as truth.[36]

One hypothesis in the doctrinal literature is that cognitive operations are more effective against pluralistic societies because such societies present more exploitable cleavages.[37] The empirical evidence for this hypothesis is mixed.

---

[33] Seumas Miller, "Cognitive Warfare: An Ethical Analysis," *Ethics and Information Technology* 25, no. 3 (2023): article 46, 8, https://doi.org/10.1007/s10676-023-09717-7.

[34] Marie Morelle, Julien Cegarra, Damien Marion, and Jean-Marc André, "Towards a Definition of Cognitive Warfare," Conference on Artificial Intelligence for Defense, Rennes, France, November 2023, 2, https://hal.science/hal-04328461v1.

[35] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 421.

[36] Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (2012): 106–31, 113, https://doi.org/10.1177/1529100612451018.

[37] Julie Ricard, Ivette Yañez, and Leticia Hora, "A Framework for Information Disorder: Modeling Mechanisms and Implications Based on a Systematic Literature Review," arXiv:2504.12537, April 16, 2025, 6, https://arxiv.org/abs/2504.12537.

Ukraine's sustained societal resilience under one of the largest documented Russian cognitive campaigns is a notable counterexample [38] and suggests that pluralism per se may matter less than the presence or absence of trusted domestic institutions and prepared strategic communication. Narrative inversion, false equivalencies, and identity-based appeals allow actors such as Russia and China to blend cognitive interference with other dimensions of hybrid warfare (diplomatic, economic, and cyber), creating compound effects that are difficult to isolate or counter.[39] These operations not only blur the lines between war and peace but also render traditional security paradigms inadequate, as the primary targets are not physical assets or military capabilities but the cognitive coherence and institutional resilience of societies themselves.

Based on the analysis of the tactics currently employed by state and non-state actors, we propose a structured "Taxonomy of Tactics Used in Cognitive Warfare" (Table 1). The taxonomy systematizes the recurring tactical patterns observed across diverse operational contexts and reflects the integrated use of disinformation, algorithmic manipulation, identity-based polarization, and other psychologically oriented tools that adversaries employ to destabilize societies from within. Each tactic is examined in relation to its strategic intent, operational mechanisms, and claimed impact on national security and democratic resilience, along with the extent to which observable evidence actually supports that impact.

By organizing these tactics into a coherent framework, the taxonomy serves as both an analytical tool and a starting point for developing countermeasures. It contributes to a more precise understanding of how cognitive threats function, how they interact with broader hybrid warfare strategies, and why they present a growing challenge to liberal democratic systems. It thus provides a step toward anticipating, detecting, and mitigating the effects of cognitive warfare in a digitally interconnected and strategically contested world.

Building on the identified tactics and their claimed implications for democratic resilience, we can also create a graphical visualization (Figure 1) in which the connections represent the relations between the two categories as documented in the case-study literature, although the strength of empirical support for these connections varies considerably across cases. Each arrow shows how a specific tactic (such as disinformation, symbolic violence, or synthetic media) is associated with vulnerabilities such as institutional delegitimization, radicalization, or fragmentation of public discourse, not a demonstrated causal relationship in every case.

---

[38] Marta Naumova, "Media Literacy Index of Ukrainians: 2020–2025 (Sixth Wave)," *Detector Media*, March 16, 2026, https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2025-sixth-wave.

[39] Nikoula and McMahon, "Cognitive Warfare: Securing Hearts and Minds," 4-6.

Table 1. Taxonomy of Tactics Used in Cognitive Warfare.

Tactic and Definition	Primary Goal and Intended Impact	Primary Tools	Observable Effect (per current evidence)
Disinformation and Strategic Deception [40] Deliberate creation and dissemination of false or misleading information to deceive and manipulate target audiences	*Goal:* Undermine trust in information sources, provoke confusion, and foster polarization *Impact:* Erosion of institutional trust, increased societal division, reduced capacity for informed public discourse	Fake news, fabricated events, troll farms, narrative inversion, and state-controlled media	Reinforces distrust mainly among already-skeptical audiences rather than creating new distrust; measurable belief change is not established
Algorithmic Amplification and Content Engineering [41] Manipulation of digital platform algorithms to prioritize polarizing or misleading content	*Goal:* Maximize dissemination of emotionally charged content to influence public opinion *Impact:* Distorted public discourse, reinforcement of echo chambers, undermined social cohesion	Engagement-driven algorithms, botnets, content curation exploits	Reach and engagement are well documented; engagement is not equivalent to belief change, and existing echo chambers are reinforced rather than newly created
Psychographic Targeting and Microprofiling [42]	*Goal:* Exploit cognitive biases and emotional triggers	Big data analytics, AI-	Persuasive effects on political attitudes/behavior

[40] Rid, *Active Measures: The Secret History of Disinformation*, 389-390; Reczkowski and Lis, "Cognitive Warfare: What Is Our Actual Knowledge?" 53; Oliver Backes and Andrew Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States" (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019), 6, https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf.

[41] Ferenc Huszár et al., "Algorithmic Amplification of Politics on Twitter," *Proceedings of the National Academy of Sciences* 119, no. 1 (2022): e2025334119, https://doi.org/10.1073/pnas.2025334119; Yvonne R. Masakowski and Janet M. Blatny, eds., *Mitigating and Responding to Cognitive Warfare*, STO Technical Report TR-HFM-ET-356 (Paris: NATO Science and Technology Organization, 2023), 58, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$$TR-HFM-ET-356-ALL.pdf; Miller, "Cognitive Warfare: An Ethical Analysis," 1.

[42] Rid, *Active Measures: The Secret History of Disinformation*, 401; Alvaro Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," preprint,

Tactic and Definition	**Primary Goal and Intended Impact**	**Primary Tools**	**Observable Effect** (per current evidence)
Use of behavioral and psychological data to craft personalized persuasive content	to shape individual behavior *Impact:* Subtle manipulation of beliefs, weakened individual autonomy, covert behavioral influence	driven profiling, microtargeted political ads	remain empirically contested; targeted interactions have not been shown to shift measured attitudes
Deepfakes and Synthetic Media Manipulation [43] Deployment of AI-generated content to mimic real individuals or events	*Goal:* Discredit opponents, fabricate realities, and confuse audiences *Impact:* Blurring of reality, damaged credibility of legitimate actors, reduced information reliability	Deepfake videos, AI-generated audio/ text, synthetic personas	Short-term confusion and virality are documented; durable shifts in belief or behavior specifically attributable to synthetic media remain sparsely evidenced
Identity-Based Polarization and Sociocultural Exploitation [44] Exploitation of identity-based divisions to destabilize social harmony	*Goal:* Fracture societal unity by mobilizing group-based grievances *Impact:* Increased polarization, reduced national cohesion, vulnerability to radicalization	Ethnic/ religious narratives, ingroup/ outgroup messaging, historical grievance activation	Operations appear to activate and amplify preexisting grievances rather than manufacture new divisions; effectiveness is contingent on prior societal cleavages

version 2, OSF Preprints, July 10, 2025, 6, https://doi.org/10.31234/osf.io/zgsej_v2; Miller, "Cognitive Warfare: An Ethical Analysis," 2.

[43] Bobby Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107 (2019): 1758, www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security; Morelle et al., "Towards a Definition of Cognitive Warfare," 4; Masakowski and Blatny, eds., *Mitigating and Responding to Cognitive Warfare*, 59.

[44] Backes and Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," 6; Nikoula and McMahon, "Cognitive Warfare: Securing Hearts and Minds," 13; Burda, *Cognitive Warfare as Part of Society*, 13.

Tactic and Definition	Primary Goal and Intended Impact	Primary Tools	Observable Effect (per current evidence)
Psychological Operations and Emotional Manipulation [45] Shaping emotions and perceptions to alter attitudes and decision-making	*Goal:* Induce fear, demoralize targets, and reduce resistance *Impact:* Reduced critical engagement, destabilized morale, and impaired judgment	Outrage engineering, fear campaigns, cognitive overload	Case-specific short-term effects are documented; sustained demoralization at a societal level is harder to establish, and resilient cases are a notable counterexample
Cognitive Fatigue and Epistemic Erosion [46] Prolonged exposure to conflicting or false information to weaken cognitive resilience	*Goal:* Overload cognitive processing and increase susceptibility to misinformation *Impact:* Lowered critical thinking, acceptance of falsehoods, confusion about what is true	Information saturation, repetitive messaging, contradictory narratives	Tactical/ operational utility is documented; durable strategic-level paralysis or disarray is less clearly evidenced, and effects appear to complement rather than substitute for kinetic outcomes
Hybrid Integration of Kinetic and Cognitive Tools [47] Coordinated use of physical and cogni-	*Goal:* Exploit confusion and paralyze response through synchronized operations *Impact:* Blurring of conflict boundaries,	Cyberattacks, synchronized propaganda, military pressure with disinformation	Cognitive and kinetic operations are documented as complementary; evidence of the cognitive component alone

[45] Todd C. Helmus et al., Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe, Research Report RR-2237-OSD (Santa Monica, CA: RAND Corporation, 2018), 16, https://doi.org/10.7249/RR2237; Rid, *Active Measures: The Secret History of Disinformation*, 389-390; Marco Marsili, "Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse," *Applied Cybersecurity & Internet Governance* 2, no. 1 (2023): 105-20, 109, https://doi.org/10.60097/ACIG/162861.

[46] Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," 113-115; Lisa K. Fazio et al., "Knowledge Does Not Protect against Illusory Truth," *Journal of Experimental Psychology: General* 144, no. 5 (2015): 993–1002, 996, 1000, https://doi.org/10.1037/xge0000098; Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," 8.

[47] Burda, *Cognitive Warfare as Part of Society*, 8; Nikoula and McMahon, "Cognitive Warfare: Securing Hearts and Minds," 7; Morelle et al., "Towards a Definition of Cognitive Warfare," 3.

Tactic and Definition	Primary Goal and Intended Impact	Primary Tools	Observable Effect (per current evidence)
tive means to maximize strategic disruption	strategic disarray, reduced response capability		producing strategic paralysis or measurable behavioral change is limited

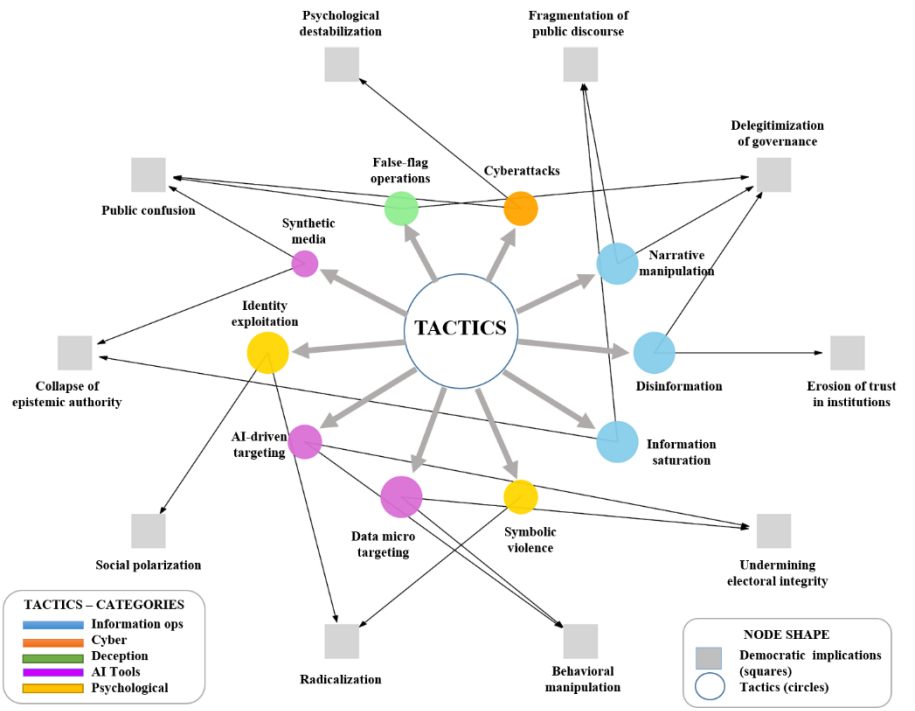

Figure 1: Associations between Cognitive Warfare Tactics and Vulnerabilities in Democratic Resilience.

Real-World Examples of Cognitive Warfare and Its Effects on Society

Cognitive warfare (CW) is the weaponization of perception, emotion, and belief systems to fracture societies and achieve strategic objectives without conventional force. Engineered narratives, from the Gulf of Tonkin incident to the public justifications for the U.S. invasions of Iraq and Afghanistan, reveal a long history

of curated information being used to mobilize support and reframe accountability.[48]

One of the largest documented cognitive campaigns of the past decade has accompanied Russia's full-scale invasion of Ukraine since 2022, and its measurable effects are instructive. The campaign combined kinetic aggression with sustained disinformation, psychological destabilization, and societal targeting. Its intended effects (the collapse of Ukrainian morale, the fragmentation of Ukrainian civil society, and the discouragement of Western support) have largely failed. This failure is itself informative: the effects of sustained cognitive operations depend heavily on the receiving society's pre-existing institutional trust and strategic-communication preparation, and they are far less deterministic than the doctrinal literature implies.

Ukraine's response to these campaigns has underscored the defensive dimension of cognitive warfare. The sustained psychological resistance of the Ukrainian population, marked by high levels of trust in leadership and widespread civic mobilization, was not accidental. It reflected a deliberate effort to prepare societal and institutional defenses, including strategic-communication training, information-hygiene campaigns, and civilian engagement in state messaging. President Zelensky's consistent public presence and symbolic leadership became focal points of national morale. They countered attempts to erode public confidence and showed that cognitive resilience can safeguard against psychological subversion.[49]

The 2014 annexation of Crimea illustrates cognitive operations achieving strategic objectives with minimal kinetic resistance: Russian actors manipulated historical narratives and cultural symbols to reframe the legitimacy of their actions and neutralize opposition before military engagement began.[50]

Table 2 summarizes a set of documented cases in which these tactics have been applied, alongside their claimed democratic and security implications and the degree to which observable evidence actually supports those implications. The set includes the longer-run pattern some scholars term "digital colonization": the sustained reshaping of a population's values and information environment by an external actor.

In conclusion, cognitive warfare's operational logic rests on its claimed ability to alter mental states, shape societal behavior, and redirect strategic decision-making without conventional force. As Table 2 and Figure 1 indicate, however, the empirical support for this claim varies considerably by case, and the observed effects are often better understood as the reinforcement of pre-existing vulnerabilities than as the creation of new ones.

---

[48] Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," 5.

[49] Liqiang Wang and Ruonan Wang, "Cyber Warfare: A Study of Zelenskyy's Social Media Political Performance Strategies and Effects," *Frontiers in Psychology* 15 (2024): 1478639, https://doi.org/10.3389/fpsyg.2024.1478639.

[50] Reczkowski and Lis, "Cognitive Warfare: What Is Our Actual Knowledge?" 58.

Table 2. Cognitive Warfare Examples.

Example and Year	Tactics and Intended Implications	Observable Outcome	Actors Involved
Russia in the Baltic States *Year:* 2014–present	*Tactics:* Disinformation, ethnic identity manipulation, narrative framing *Implications:* Undermining institutional legitimacy, eroding trust among minorities	Narrative reach among Russian-speaking minorities is documented; no rigorous evidence of measurable shifts in institutional trust or electoral behavior at the population level	Russian state media, intelligence agencies
Russia in Ukraine: pre-invasion operations *Year:* 2021–2022	*Tactics:* Cyberattacks, false-flag operations, narrative flooding *Implications:* Public confusion, psychological destabilization, justification for invasion	Operations are well documented; a causal link to durable public confusion or destabilization, as opposed to short-term disruption, has not been established	Russian GRU, troll farms
Russia in Ukraine: digital dossiers *Year:* 2022	*Tactics:* Data harvesting, targeted intimidation, psychological terror *Implications:* Fear, leader elimination, disruption of community cohesion	Tactical/operational use is documented; no rigorous evidence that the campaign produced the intended societal-level fear or breakdown of cohesion	Russian intelligence, military units
COVID-19 Infodemic *Year:* 2020–2022	*Tactics:* Disinformation on health measures, conspiracy amplification *Implications:* Public health disobedience, erosion of scientific authority, social fragmentation	An association between disinformation exposure and vaccine hesitancy is documented in some studies; causal attribution to specific foreign operations, rather than the general online misinformation ecosystem, remains contested	Multiple state and non-state actors (including Russia, China, and conspiracy groups)
Canada Freedom Convoy Protests *Year:* 2022	*Tactics:* Foreign amplification of cultural tensions, narrative distortion	Foreign amplification of the protest narrative is documented; the protest's origins and	Russian state-linked media, online

Example and Year	Tactics and Intended Implications	Observable Outcome	Actors Involved
	Implications: Delegitimization of government response, increased polarization	momentum were substantially domestic, and the independent causal contribution of amplification has not been isolated	activist networks
Islamic State (ISIS) *Year:* 2014–2019	*Tactics:* Digital propaganda, symbolic violence, recruitment through narrative manipulation *Implications:* Radicalization, transnational recruitment, erosion of state legitimacy	This is among the better-evidenced cases, with documented foreign-fighter recruitment flows; effects were concentrated among individuals with pre-existing grievances rather than the general population	ISIS media units
French Parliamentary Disruption *Year:* 2023	*Tactics:* Fake emergency messages targeting lawmakers *Implications:* Disruption of legislative processes, emotional destabilization of decision-makers	Operational disruption is documented; however, evidence of lasting destabilization of legislative decision-making is limited	Unknown (suspected Russian interference)
Mali Wagner Group Operations *Year:* 2021–2023	*Tactics:* Staged atrocities, disinformation to discredit foreign forces *Implications:* Erosion of foreign military legitimacy, shifting local alliances	A documented shift in alliances did occur, making this one of the more clearly "successful" cases; disentangling disinformation's specific causal contribution from military and political factors is difficult	Wagner Group, Russian media channels
U.S. 2020 Elections (Russia/ Cambridge Analytica) *Year:* 2016–2020	*Tactics:* Microtargeting via social media, data analytics, narrative manipulation *Implications:* Voter behavior manipulation, undermining electoral trust	Bail et al. found no measurable effect of IRA-account interaction on six distinct attitude/ behavior measures; evidence	Russian Internet Research Agency, Cambridge Analytica

Example and Year	Tactics and Intended Implications	Observable Outcome	Actors Involved
		points to reinforcement rather than attitude change	
Romanian Presidential Election *Year:* 2024–2025	*Tactics:* TikTok algorithmic favoritism, coordinated inauthentic networks, covert paid promotion *Implications:* Election of a pro-Russian candidate, delegitimization of pro-Western governance	Documented network activity was cited by the Constitutional Court in annulling the 2024 result; a different far-right candidate still received 41 % of the vote in the first round of the 2025 rerun, consistent with reinforcement rather than newly formed sentiment	Russian-linked networks, platform algorithms

AI-Driven Influence Operations and Big Data Analytics Transform the Cognitive Battlespace

The fusion of artificial intelligence (AI), machine learning, and big data analytics has transformed the cognitive battlespace, enabling influence operations that are scalable, hyper-personalized, and persistent in their psychological effects over time and across digital environments.[51] By using predictive behavioral profiling and sentiment analysis, adversaries can adapt persuasive content dynamically and tailor it with unprecedented precision to the ideological, emotional, and cultural predispositions of individuals or communities.[52] These algorithmically curated interactions can reinforce cognitive biases and create a self-reinforcing system of influence that refines its strategies in real time, potentially blurring the line between genuine public discourse and engineered psychological manipulation.[53]

Recent monitoring, however, complicates the picture of an unchecked AI advantage. OpenAI's "Disrupting Malicious Uses of AI" reports (2025–2026) describe campaigns originating in or linked to Russia, China, and Iran, including a

[51] Masakowski and Blatny, eds., *Mitigating and Responding to Cognitive Warfare*, 64; Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," 7.

[52] Reczkowski and Lis, "Cognitive Warfare: What Is Our Actual Knowledge?" 53; Marsili, "Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse," 116.

[53] Morelle et al., "Towards a Definition of Cognitive Warfare," 2; Nikoula and McMahon, "Cognitive Warfare: Securing Hearts and Minds," 8-9.

2026 network operating through a fabricated think tank.[54] These operations are repeatedly assessed as reaching limited audiences with low real-world impact, which is consistent with this article's argument.

In conclusion, the convergence of AI, big data analytics, and automated content generation has redefined the parameters of influence in the cognitive battlespace. It has made possible a mode of engagement that is algorithmically orchestrated, persistently adaptive, and potentially destabilizing.[55,56] As the capacity for highly personalized psychological operations continues to grow, so does the strategic imperative to understand and counter their cognitive, social, and political consequences. Without robust regulatory frameworks and a shift toward anticipatory defense strategies, democratic societies remain vulnerable to a form of warfare that, though largely invisible, may shape the future of cognition and conflict.

Building Societal Resilience: National Responses to Cognitive Threats

To counteract cognitive warfare, societal resilience must be built across multiple levels, incorporating educational, governmental, and technological approaches. Unlike traditional cybersecurity, which focuses on technological vulnerabilities, cognitive resilience requires an understanding of the social and psychological factors that influence how people interpret information and form beliefs.

Countermeasures carry ethical stakes. Defense architectures must preserve cognitive autonomy when countering AI-enhanced influence operations; otherwise, societies risk reproducing the very forms of manipulation they seek to resist).[57]

A stark asymmetry separates democratic responses from the centralized and unapologetically manipulative approaches of authoritarian regimes such as China and Russia. These states maintain enduring cognitive strategies that treat psychological operations as a routine and legitimate instrument of statecraft, leveraging tightly controlled information ecosystems and state-sponsored disinformation infrastructures. Operating with few legal or normative constraints,

[54] OpenAI, "Disrupting Malicious Uses of AI," February 25, 2026, https://openai.com/index/disrupting-malicious-ai-uses/; SC Staff, "OpenAI Disrupts Russian-Linked AI Influence Campaign Targeting Western Audiences," *SC Media*, August 27, 2026, www.scworld.com/brief/openai-disrupts-russian-linked-ai-influence-campaign-targeting-western-audiences.

[55] Morelle et al., "Towards a Definition of Cognitive Warfare," 4; Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," 6.

[56] Lance Y. Hunter et al., "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations," *Defense & Security Analysis* 40, no. 2 (2024): 235–69, 250–51, https://doi.org/10.1080/14751798.2024.2321736.

[57] Pastor, "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour," 10; Miller, "Cognitive Warfare: An Ethical Analysis," 2.

these regimes integrate AI, surveillance, and information control into their security architecture, enabling persistent influence operations that exploit the openness of liberal systems.[58]

Ukraine offers a revealing contrast, demonstrating the potential of adaptive, decentralized, and participatory models of information defense. Since 2014, Ukraine has cultivated societal resilience through coordinated efforts across civil society, media organizations, and public institutions to combat Russian disinformation and preserve national cohesion. Civic mobilization, supported by strategic collaborations with private technology firms and international allies, has enabled effective counter-narratives and operational continuity. Nonetheless, challenges remain, particularly regarding the influence of foreign technology platforms and the amplification of adversarial narratives by opaque algorithmic systems.[59]

Comparative assessments of responses in Ukraine, Finland, and the Baltic states suggest that the most effective strategies are anticipatory, integrative, and socially inclusive. Finland's incorporation of media literacy into its national education curriculum, Estonia's attention to ethnic minority integration, and Lithuania's fusion of public and private sector capabilities exemplify comprehensive approaches to cognitive defense. These contrast sharply with more reactive or siloed models, in which cognitive threats are addressed only after strategic damage has occurred.[60]

The resilience of societies against cognitive warfare hinges on their capacity to detect, mitigate, and recover from information-based threats. Among the most significant long-term solutions is the integration of media literacy and critical thinking within national education systems. Experimental evidence (for example, the inoculation-theory studies or the field experiment of Guess et al.) shows that individuals exposed to structured media-literacy interventions display measurably improved discrimination of manipulated content. Effect sizes are typically modest and decay without booster interventions,[61] consistent with the broader argument developed here that resilience is a distributed institutional property rather than a purely individual capacity. Programs that cultivate media literacy and teach citizens to distinguish between credible information

[58] Hunter et al., "Artificial Intelligence and Information Warfare in Major Power States," 254; Marsili, "Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse," 115-116.

[59] Keir Giles, *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*, Research Paper (London: Chatham House, December 2023), 51, www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice.

[60] Burda, *Cognitive Warfare as Part of Society*, 9; Backes and Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," 10.

[61] OECD, *Facts Not Fakes: Tackling Disinformation, Strengthening Information Integrity* (Paris: OECD Publishing, March 2024), 83, https://doi.org/10.1787/d909ff7a-en; Rakoen Maertens et al., "Psychological Booster Shots Targeting Memory Increase Long-Term Resistance against Misinformation," *Nature Communications* 16, no. 1 (2025): 2062, 9–10, https://doi.org/10.1038/s41467-025-57205-x.

and manipulated content can improve discernment and reduce susceptibility to disinformation.[62] Nordic countries provide illustrative examples, having embedded media literacy education at multiple levels, which is associated with higher societal resistance to foreign influence campaigns.[63]

Institutional reforms must also address the evolving digital battlespace. Regulatory instruments such as the European Union's "Code of Conduct on Disinformation" and the Digital Services Act mark important steps toward improving transparency and platform accountability. The EU's separate regulation on political advertising sets specific transparency requirements for political ads. While regulatory measures alone cannot neutralize cognitive threats, they help to construct a more secure information ecosystem by curbing the reach of manipulative content and holding technology platforms accountable for the information they amplify.[64,65]

The most operationally mature European effort to detect and respond to cognitive-warfare-adjacent operations is the European External Action Service (EEAS) series of Reports on Foreign Information Manipulation and Interference (FIMI) Threats. The first report (2023) established the FIMI Methodology, a standardized analytical framework for FIMI investigations.[66] The second report (2024) developed the FIMI Response Framework, which links analysis to timely, coordinated responses, and illustrated its use through an analysis of 33 election-related incidents.[67]

---

[62] Stephan Lewandowsky, Ullrich K. H. Ecker, and John Cook, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," *Journal of Applied Research in Memory and Cognition* 6, no. 4 (2017): 353–69, 363, https://doi.org/10.1016/j.jarmac.2017.07.008; Andrew M. Guess et al., "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India," *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536–45, 15536, https://doi.org/10.1073/pnas.1920498117.

[63] Daniel Funke, "Global Responses to Misinformation and Populism," in *The Routledge Companion to Media Disinformation and Populism*, ed. Howard Tumber and Silvio Waisbord (London: Routledge, 2021), 455, https://doi.org/10.4324/9781003004431.

[64] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), *Official Journal of the European Union* L 277 (October 27, 2022): 59, art. 26, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065.

[65] European Commission, "The Code of Conduct on Disinformation," Shaping Europe's Digital Future, February 13, 2025, 15, 21, 31–32, https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

[66] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence* (Brussels: EEAS, February 2023), 5, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

[67] European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence* (Brussels: EEAS, January 2024), 23, www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.

The third report (2025) introduced the FIMI Exposure Matrix to support the identification and attribution of FIMI infrastructure.[68] It analyzed 505 FIMI incidents from November 4, 2023, to November 4, 2024, involving 38,000 unique channels. The incidents targeted 322 organizations and 90 countries. The fourth report (2026) documented 540 FIMI incidents in 2025, 29 % of them attributed to Russia, and consolidated the FIMI Toolbox and the FIMI Deterrence Playbook as instruments to make FIMI activity more costly and less sustainable for perpetrators.[69] Together, the four reports provide both empirical data on the scale of attempted operations and a maturing operational vocabulary for response; they are the natural reference point for any Euro-Atlantic cognitive-security strategy.

Ultimately, cognitive resilience is neither purely defensive nor merely reactive. It is a multidimensional, anticipatory posture grounded in normative clarity, technological innovation, and civic participation. To preserve democratic sovereignty in the information age, societies must embed cognitive defense in their institutional, educational, and ethical infrastructures. The strategic contest of the twenty-first century is not merely over territory or resources; it is over attention, belief, and trust.

Future Challenges and Recommendations

As cognitive warfare tactics continue to evolve, future challenges will require adaptive, forward-looking strategies. The rapid advancement of AI, quantum computing, and neurotechnology opens new dimensions of the information battlespace. AI-assisted disinformation campaigns, which can produce highly persuasive and contextually adaptive content, pose a serious threat to democratic resilience. Research suggests that deep learning models can generate "neural fake news," propaganda that closely mimics the style of real news and that readers may find as credible as human-written text, which complicates efforts to counteract cognitive manipulation.[70] Furthermore, breakthroughs in neurotechnology could in future enable more sophisticated forms of cognitive manipulation that influence perception and behavior more directly.[71]

---

[68] European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (Brussels: EEAS, March 2025), 5, https://eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en.

[69] European External Action Service, *4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards* (Brussels: EEAS, March 2026), 16–23, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web.pdf.

[70] Rowan Zellers et al., "Defending against Neural Fake News," paper presented at the 33rd Conference on Neural Information Processing Systems (NeurIPS 2019), Vancouver, Canada, December 2019, https://papers.neurips.cc/paper_files/paper/2019/file/3e9f0fc9b2f89e043bc6233994dfcf76-Paper.pdf.

[71] Martha J. Farah, "Neuroethics: The Ethical, Legal, and Societal Impact of Neuroscience," *Annual Review of Psychology* 63 (2012): 571–91, 585, https://doi.org/10.1146/annurev.psych.093008.100438.

To address these challenges, policymakers and defense strategists must prioritize three areas. First, investment in research and development on cognitive resilience is essential. Interdisciplinary studies that integrate psychology, cybersecurity, and AI ethics can show which countermeasures work. Second, closer international cooperation within NATO and allied frameworks can facilitate the sharing of intelligence and best practices in cognitive defense. Finally, transparent governance and credible communication can foster civic engagement and trust in institutions, and so strengthen societal resilience against manipulation. Without such measures, societies will remain vulnerable to adversarial cognitive operations that seek to erode the foundations of stability and governance.

Conclusion

The challenge posed by cognitive warfare is not only technological or strategic, but also fundamentally epistemological and ethical. At its core, cognitive warfare aims to destabilize the processes by which individuals and societies determine what is true. This poses a profound risk to democratic governance, which depends on a shared commitment to reasoned discourse, transparency, and mutual recognition.

The ethical questions are equally significant. Defensive cognitive operations (such as counter-propaganda or behavioral nudging) raise concerns about manipulation, autonomy, and democratic consent. Where is the line between resilience-building and coercion? Who defines legitimate influence? These questions remain largely unresolved.

While recent efforts to build cognitive resilience through media literacy, algorithmic transparency, and public-private partnerships are promising, they are not sufficient. What is required is a broader normative framework that treats cognitive integrity as a public good and embeds ethical safeguards into both civilian and military information environments.

Disclaimer

The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Partnership for Peace Consortium, its participating institutions, or any governmental or international organizations affiliated with its governance structure.

About the Author

Colonel **Cezar Vasilescu**, PhD Habil, BEng, is a professor at the Regional Department of Defense Resources Management Studies (DRESMARA) in Brașov, part of the "Carol I" National Defence University. He has served as director of DRESMARA's Postgraduate School of Studies and supervises doctoral research in military science. He graduated from the Air Force Academy in Brașov and earned a PhD in engineering sciences, specializing in computer science, from the Military Technical Academy in Bucharest. He completed the Advanced Management Program at the US National Defense University and holds Chief Information Officer certification from the US Department of Defense. His research covers cybersecurity, critical infrastructure protection, and hybrid threats. He contributes to NATO's Defence Education Enhancement Programme (DEEP), serves as a visiting expert in cyber defense within NATO's Cyberspace Operations Discipline, and is editor-in-chief of the *Journal of Defense Resources Management*.
https://orcid.org/0000-0002-5280-8795; *E-mail*: cvasilescu1@mapn.ro

Bibliography

Altay, Sacha, Manon Berriche, and Alberto Acerbi. “Misinformation on Misinformation: Conceptual and Methodological Challenges.” *Social Media + Society* 9, no. 1 (2023). https://doi.org/10.1177/20563051221150412.

Backes, Oliver, and Andrew Swab. *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019. https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf.

Bail, Christopher A., et al. “Assessing the Russian Internet Research Agency’s Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017.” *Proceedings of the National Academy of Sciences* 117, no. 1 (2020): 243–250. https://doi.org/10.1073/pnas.1906420116.

Bourbeau, Philippe. “Resiliencism: Premises and Promises in Securitisation Research.” *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013): 3–17. https://doi.org/10.1080/21693293.2013.765738.

Burda, Robin. *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds*. The Hague: The Hague Centre for Strategic Studies, June 2023. https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf.

Cao, Kathy, et al. “Countering Cognitive Warfare: Awareness and Resilience.” *NATO Review*, May 20, 2021. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

Chandler, David. *Resilience: The Governance of Complexity*. Abingdon: Routledge, 2014.

Chesney, Bobby, and Danielle Keats Citron. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107 (2019): 1753–1820. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security.

Claverie, Bernard, and François du Cluzel. “The Cognitive Warfare Concept.” NATO Allied Command Transformation Innovation Hub, 2022. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

Deppe, Christoph, and Gary S. Schaal. “Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept.” *Frontiers in Big Data* 7 (2024): 1452129. https://doi.org/10.3389/fdata.2024.1452129.

Dragolov, Georgi, et al. *Social Cohesion Radar – Measuring Common Ground: An International Comparison of Social Cohesion, Methods Report*. Gütersloh: Bertelsmann Stiftung, 2013. https://aei.pitt.edu/74134/1/Social_cohesion_radar.pdf.

du Cluzel, François. “Cognitive Warfare, a Battle for the Brain.” Keynote 3 in *Mitigating and Responding to Cognitive Warfare*. STO-MP-HFM-334. Paris: NATO Science and Technology Organization, 2022. https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf.

Durkheim, Émile. *The Division of Labor in Society*. Translated by George Simpson. New York: Macmillan, 1933.

European Commission. *2025 Strategic Foresight Report – Resilience 2.0: Empowering the EU to Thrive Amid Turbulence and Uncertainty*. COM(2025) 484 final. Brussels: European Commission, September 9, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0484.

European Commission. “The Code of Conduct on Disinformation.” *Shaping Europe’s Digital Future*, February 13, 2025. https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

European External Action Service. *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence*. Brussels: EEAS, February 2023. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

European External Action Service. *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*. Brussels: EEAS, January 2024. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.

European External Action Service. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations*. Brussels: EEAS, March 2025. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

European External Action Service. *4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards*. Brussels: EEAS, March 2026. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web.pdf.

Farah, Martha J. “Neuroethics: The Ethical, Legal, and Societal Impact of Neuroscience.” *Annual Review of Psychology* 63 (2012): 571–591. https://doi.org/10.1146/annurev.psych.093008.100438.

Fazio, Lisa K., et al. “Knowledge Does Not Protect against Illusory Truth.” *Journal of Experimental Psychology: General* 144, no. 5 (2015): 993–1002. https://doi.org/10.1037/xge0000098.

Funke, Daniel. “Global Responses to Misinformation and Populism.” In *The Routledge Companion to Media Disinformation and Populism*, edited by Howard

Tumber and Silvio Waisbord. London: Routledge, 2021. https://doi.org/10.4324/9781003004431.

Giles, Keir. *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*. Research Paper. London: Chatham House, December 2023. https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice.

Guess, Andrew M., et al. "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India." *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536–15545. https://doi.org/10.1073/pnas.1920498117.

Helmus, Todd C., et al. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Research Report RR-2237-OSD. Santa Monica, CA: RAND Corporation, 2018. https://doi.org/10.7249/RR2237.

Hung, Tzu-Chieh, and Tzu-Wei Hung. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." *Journal of Global Security Studies* 7, no. 4 (2022): ogac016. https://doi.org/10.1093/jogss/ogac016.

Hunter, Lance Y., et al. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." *Defense & Security Analysis* 40, no. 2 (2024): 235–269. https://doi.org/10.1080/14751798.2024.2321736.

Huszár, Ferenc, et al. "Algorithmic Amplification of Politics on Twitter." *Proceedings of the National Academy of Sciences* 119, no. 1 (2022): e2025334119. https://doi.org/10.1073/pnas.2025334119.

Levi, Margaret. "A State of Trust." In *Trust and Governance*, edited by Valerie A. Braithwaite and Margaret Levi. New York: Russell Sage Foundation, 1998.

Lewandowsky, Stephan, Ullrich K. H. Ecker, and John Cook. "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era." *Journal of Applied Research in Memory and Cognition* 6, no. 4 (2017): 353–369. https://doi.org/10.1016/j.jarmac.2017.07.008.

Lewandowsky, Stephan, et al. "Misinformation and Its Correction: Continued Influence and Successful Debiasing." *Psychological Science in the Public Interest* 13, no. 3 (2012): 106–131. https://doi.org/10.1177/1529100612451018.

Libicki, Martin C. *What Is Information Warfare?* Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995. https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf.

Lorenz-Spreen, Philipp, et al. “A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy.” *Nature Human Behaviour* 7, no. 1 (2023): 74–101. https://doi.org/10.1038/s41562-022-01460-1.

Maertens, Rakoen, et al. “Psychological Booster Shots Targeting Memory Increase Long-Term Resistance against Misinformation.” *Nature Communications* 16, no. 1 (2025): 2062. https://doi.org/10.1038/s41467-025-57205-x.

Marsili, Marco. “Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse.” *Applied Cybersecurity & Internet Governance* 2, no. 1 (2023): 105–120. https://doi.org/10.60097/ACIG/162861.

Masakowski, Yvonne R., and Janet M. Blatny, eds. *Mitigating and Responding to Cognitive Warfare*. STO Technical Report TR-HFM-ET-356. Paris: NATO Science and Technology Organization, 2023. https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$$TR-HFM-ET-356-ALL.pdf.

Matheson, Jonathan. “The Philosophy of Epistemic Autonomy: Introduction to Special Issue.” *Social Epistemology* 38, no. 3 (2024): 267–273. https://doi.org/10.1080/02691728.2024.2335623.

Miller, Seumas. “Cognitive Warfare: An Ethical Analysis.” *Ethics and Information Technology* 25, no. 3 (2023): article 46. https://doi.org/10.1007/s10676-023-09717-7.

Morelle, Marie, et al. “Towards a Definition of Cognitive Warfare.” Paper presented at the Conference on Artificial Intelligence for Defense, DGA Maîtrise de l’Information, Rennes, France, November 2023. https://hal.science/hal-04328461v1.

NATO Allied Command Transformation. “Cognitive Warfare.” Accessed July 29, 2025. https://www.act.nato.int/activities/cognitive-warfare.

Naumova, Marta. “Media Literacy Index of Ukrainians: 2020–2025 (Sixth Wave).” *Detector Media*, March 16, 2026. https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2025-sixth-wave.

Nikoula, Daniel, and Dave McMahon. *Cognitive Warfare: Securing Hearts and Minds*. Ottawa: Information Integrity Lab, University of Ottawa, July 2024. https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf.

Norris, Pippa. *Democratic Deficit: Critical Citizens Revisited*. New York: Cambridge University Press, 2011.

OECD. *Facts Not Fakes: Tackling Disinformation, Strengthening Information Integrity*. Paris: OECD Publishing, March 2024. https://doi.org/10.1787/d909ff7a-en.

OpenAI. "Disrupting Malicious Uses of AI." February 25, 2026. https://openai.com/index/disrupting-malicious-ai-uses/.

Pastor, Alvaro. "Cognitive Warfare: The Weaponisation of the Science of Brain and Behaviour." Preprint, version 2. OSF Preprints, July 10, 2025. https://doi.org/10.31234/osf.io/zgsej_v2.

Reczkowski, Robert, and Andrzej Lis. "Cognitive Warfare: What Is Our Actual Knowledge and How to Build State Resilience?" *Bezpieczeństwo. Teoria i Praktyka (Security Theory and Practice)* 48, no. 3 (2022): 51–61. https://doi.org/10.48269/2451-0718-btip-2022-3-003.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union* L 277 (October 27, 2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065.

Ricard, Julie, Ivette Yañez, and Leticia Hora. "A Framework for Information Disorder: Modeling Mechanisms and Implications Based on a Systematic Literature Review." arXiv:2504.12537 [cs.CY], April 16, 2025. https://arxiv.org/abs/2504.12537.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.

Rothstein, Bo. *The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective*. Chicago: University of Chicago Press, 2011.

Rothstein, Bo, and Jan Teorell. "What Is Quality of Government? A Theory of Impartial Government Institutions." *Governance: An International Journal of Policy, Administration, and Institutions* 21, no. 2 (2008): 165–190. https://doi.org/10.1111/j.1468-0491.2008.00391.x.

SC Staff. "OpenAI Disrupts Russian-Linked AI Influence Campaign Targeting Western Audiences." *SC Media*, August 27, 2026. https://www.scworld.com/brief/openai-disrupts-russian-linked-ai-influence-campaign-targeting-western-audiences.

Wang, Liqiang, and Ruonan Wang. "Cyber Warfare: A Study of Zelenskyy's Social Media Political Performance Strategies and Effects." *Frontiers in Psychology* 15 (2024): 1478639. https://doi.org/10.3389/fpsyg.2024.1478639.

Weber, Max. *Economy and Society: An Outline of Interpretive Sociology*. Edited by Guenther Roth and Claus Wittich. Translated by Ephraim Fischoff et al. Berkeley: University of California Press, 1978.

Zellers, Rowan, et al. "Defending against Neural Fake News." Paper presented at the 33rd Conference on Neural Information Processing Systems (NeurIPS 2019), Vancouver, Canada, December 2019. https://papers.neurips.cc/paper_files/paper/2019/file/3e9f0fc9b2f89e043bc6233994dfcf76-Paper.pdf.