LUISS

Degree Program in International Relations

Course of Security Studies

Securing Strategic Communication Networks against Misinformation and Malinformation: The United States, France, and Poland from the End of the Cold War through the Rise of Artificial Intelligence

Gen. S.A. Carlo Magrassi

SUPERVISOR

Prof. Gregory Alegi

CO-SUPERVISOR

Anne-Laure Bodin (n°655552)

CANDIDATE

Academic Year 2024/2025

"In the technetronic society the trend seems to be toward aggregating the individual support of millions of unorganized citizens, who are easily within the reach of magnetic and attractive personalities, and effectively exploiting the latest communication techniques to manipulate emotions and control reason."

Zbigniew Brzezinski,
"Between Two Ages: America's Role in the Technetronic Era" (1970)

ACKNOWLEDGMENTS

This thesis would not have been possible without the guidance and support of many individuals who contributed to its development over the past two years.

I extend my deepest gratitude to my thesis supervisor, Gen. S.A. Carlo Magrassi, and co-supervisor, Prof. Gregory Alegi, whose guidance and constructive criticism throughout this research process proved invaluable. Their expertise in international relations theory and security studies helped shape this comparative analysis while challenging me to maintain analytical rigor and theoretical coherence.

I am grateful to Dr. Gianluca Scialdone and Dr. Simone Pasquazzi for their valuable assistance and feedback with this thesis. Their support and insights contributed to my understanding of the subject matter.

Ma gratitude s'étend à mes parents Gilles et Véronique, mon frère Clément et ma sœur Carla, dont la patience, les encouragements et la compréhension m'ont soutenu tout au long des défis de ces deux années de master. Leur soutien inconditionnel et leur confiance en mes capacités ont été une source de motivation constante. Leur présence a rendu possible l'achèvement de ce travail.

Enfin et non des moindres, je tiens à remercier particulièrement Jade pour son soutien incommensurable durant ces deux années d'études, de m'avoir accompagnée et soutenue tout au long de cette épreuve. Sa présence, ses encouragements et sa compréhension ont été essentiels à la réussite de ce projet académique.

Finally, I take full responsibility for any errors or shortcomings that remain in this analysis. The views expressed are my own and do not reflect the positions of any individuals who assisted with this research.

Anne-Laure

ABSTRACT

This thesis examines how the United States, France, and Poland have adapted their strategic communication networks to address misinformation and malinformation threats from 1991 to 2024, with particular focus on artificial intelligence's transformative impact. The research investigates how different institutional arrangements, strategic cultures, and threat environments shape national approaches to cognitive security governance, asking what factors determine response effectiveness in maintaining democratic legitimacy while providing adequate protection against information warfare.

The study employs a theoretical framework combining securitization theory, constructivist international relations, and resilience studies to analyze how democratic societies navigate tensions between protecting collective decision-making processes and preserving epistemic pluralism. Using a "most different systems" design, the research compares American fragmented federalism with constitutional constraints, French centralized republicanism emphasizing state-directed strategic autonomy, and Polish alliance-dependent adaptation under immediate hybrid threat exposure. The methodology combines structured focused comparison with process tracing, utilizing government documents, parliamentary testimony, declassified assessments, and expert interviews from 2022-2024.

The analysis reveals three principal findings challenging conventional assumptions about democratic information security. Institutional architecture determines response capacity more than absolute resource levels e.g. French centralized coordination achieved 4.8-hour average crisis response times compared to 18-hour averages for fragmented American approaches despite ten-fold resource disparities. Constitutional constraints create operational trade-offs rather than simple disadvantages e.g. American First Amendment protections limit domestic operations while generating compensating advantages through enhanced civil society resilience. Alliance integration enables capability sharing but creates dependency vulnerabilities, as demonstrated by Poland's reliance on NATO and EU frameworks.

The research contributes to security studies theory by developing "graduated securitization" concepts that capture how democratic societies implement extraordinary measures while maintaining accountability mechanisms. The analysis demonstrates that traditional securitization theory requires modification to account for information warfare's continuous, distributed threat construction processes.

Policy implications emphasize that effective democratic responses require constitutional adaptation rather than imported best practices, sustainable civil society investment despite funding challenges, and technology governance frameworks balancing innovation with security imperatives. The thesis concludes that democratic societies face genuine but not insurmountable challenges in adapting to information warfare while preserving constitutional character, requiring patient institution-building rather than rapid technological fixes through distinct approaches reflecting institutional constraints and threat environments.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Tables

Figure

LIST OF ABBREVIATIONS

AFP: Agence France-Presse (French Press Agency)
AI: Artificial Intelligence
AID: Agence de l'Innovation de défense (French Defense Innovation Agency)
AJP-10: Allied Joint Publication 10 (NATO Strategic Communications Joint Doctrine)
ANSSI: Agence Nationale de la sécurité des Systèmes d'Information (French National Cybersecurity Agency)
APT28: Advanced Persistent Threat 28 (Russian hacking group)
BBC: British Broadcasting Corporation
C2PA: Coalition for Content Provenance and Authenticity
CBOS: Centrum Badania Opinii Społecznej (Polish Center for Public Opinion Research)
CDC: Centers for Disease Control and Prevention (US)
CERT: Computer Emergency Response Team
CEVIPOF: Centre de Recherches Politiques de Sciences Po (Sciences Po Center for Political Research, France)
CGTN: China Global Television Network
CIA: Central Intelligence Agency (US)
CISA: Cybersecurity and Infrastructure Security Agency (US)
CLOUD Act: Clarifying Lawful Overseas Use of Data Act (US)
CNN: Cable News Network
CNIL: Commission Nationale de l'Informatique et des Libertés (French National Commission on Informatics and Liberty)
CNCCEP: Commission Nationale de Contrôle de la Campagne Électorale en vue de l'Élection Présidentielle (French National Commission for the Control of the Electoral Campaign for the Presidential Election)
CoE: Centre of Excellence
COMCYBER: Commandement de la cyberdéfense (Cyber Defense Command, France)
COVID-19: Coronavirus Disease 2019
DARPA: Defense Advanced Research Projects Agency (US)
DGSI: Direction Générale de la Sécurité Intérieure (General Directorate for Internal Security, France)
DHS: Department of Homeland Security (US)
DICoD: Délégation à l'Information et à la Communication de la Défense (Defense Information and Communication Delegation, France)
DNC: Democratic National Committee (US)
DoD: Department of Defense (US)
DSA: Digital Services Act (EU)
EU: European Union
FBI: Federal Bureau of Investigation (US)

FISA: Foreign Intelligence Surveillance Act (US)
FOIA: Freedom of Information Act (US)
FSB: Federal Security Service (Russia)
FTE: Full-Time Equivalent
GAO: Government Accountability Office (US)
GDP: Gross Domestic Product
GDPR: General Data Protection Regulation (EU)
GEC: Global Engagement Center (US)
GPT: Generative Pre-trained Transformer
GRU: лавное разведывательное управление - Glavnoye Razvedyvatel'noye Upravleniye (Main Intelligence Directorate, Russia)
IBM: International Business Machines Corporation
IED: Improvised Explosive Device
IFOP: Institut Français d'Opinion Publique (French Institute of Public Opinion)
IO/InfoOps: Information Operations
IPSOS: Institut de sondages d'opinion publique (Institute of Public Opinion Polling, France)
IRA: Internet Research Agency (Russia)
IR: International Relations
IRSEM: Institut de Recherche Stratégique de l'École Militaire (Institute for Strategic Research at the Military School, France)
ISAF: International Security Assistance Force
ISIS/ISIL: Islamic State of Iraq and Syria/Islamic State of Iraq and the Levant
ISR: Intelligence, Surveillance, and Reconnaissance
IT: Information Technology
JADC2: Joint All-Domain Command and Control (US)
KGB: Комитет государственной безопасности - Komitet Gosudarstvennoy Bezopasnosti (Committee for State Security, Soviet Union)
L2I: Lutte Informatique d'Influence (French Information Warfare)
LLM: Large Language Model
MediFor: Media Forensics (DARPA program)
MIT: Massachusetts Institute of Technology
MoD: Ministry of Defense
MSWiA: Ministry of Interior and Administration (Poland)
NATO: North Atlantic Treaty Organization
NCBC: Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (Polish National Cyber Security Centre)
NetzDG: Netzwerkdurchsetzungsgesetz (Network Enforcement Act, Germany)
NGO: Non-Governmental Organization
NIS2: Network and Information Systems Directive 2 (EU)
NIST: National Institute of Standards and Technology (US)

NSA: National Security Agency (US)
NSC: National Security Council (US)
NSO: NSO Group (Israeli surveillance company)
OECD: Organisation for Economic Co-operation and Development
OPSEC: Operations Security
OSCE: Organization for Security and Co-operation in Europe
PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
PiS: Prawo i Sprawiedliwość (Law and Justice Party, Poland)
PLN: Polish Złoty (Polish currency)
PSYOPS: Psychological Operations
RAND: Research ANd Development Corporation
RCB: Rządowe Centrum Bezpieczeństwa (Polish Government Center for Security)
RFI: Radio France Internationale (Radio France International)
RT: Russia Today
SemaFor: Semantic Forensics (DARPA program)
SGDSN: Secrétariat Général de la Défense et de la Sécurité Nationale (French General Secretariat for Defense and National Security)
SIG: Service d'Information du Gouvernement (French Government Information Service)
StratCom: Strategic Communications
TVN: Television Network (Poland)
TVP: Telewizja Polska (Polish Television)
UCLAT: Unité de Coordination de la Lutte AntiTerroriste (French Counterterrorism Coordination Unit)
UK: United Kingdom
UN: United Nations
UNESCO: United Nations Educational, Scientific and Cultural Organization
U.S./USA: United States of America
USIA: United States Information Agency
USSR: Union of Soviet Socialist Republics
V4: Visegrád Group (Czech Republic, Hungary, Poland, and Slovakia)
VIGINUM: Vigilance et protection contre les ingérences numériques étrangères (French Service for Vigilance and Protection against Foreign Digital Interference)
WHO: World Health Organization
WIPO: World Intellectual Property Organization
YLE: Yleisradio (Finnish Broadcasting Company)

INTRODUCTION

The end of the Cold War promised democratic expansion and liberal international order, yet three decades later, democratic societies confront unprecedented challenges to their foundational assumptions about information, truth, and collective decision-making. The transformation of the global information landscape since 1991 has evolved from initial optimism about digital technologies' democratizing potential into sobering recognition that these same technologies can be weaponized to undermine the democratic institutions they were expected to strengthen. What began as isolated foreign interference has crystallized into systematic cognitive warfare campaigns targeting the epistemological foundations of democratic governance itself.

This thesis examines how three democratic allies (i.e. the United States, France, and Poland) have adapted their strategic communication networks to address evolving misinformation and malinformation threats in the post-Cold War era, with particular attention to artificial intelligence's transformative impact.

How have different democratic institutional arrangements, strategic cultures, and threat environments shaped national approaches to cognitive security governance, and what factors determine the effectiveness of these responses in maintaining democratic legitimacy while providing adequate protection against information warfare?

This inquiry's significance extends far beyond comparative institutional analysis. As synthetic media technologies achieve unprecedented sophistication and AI enables automated persuasion at industrial scale, democratic societies face an existential challenge to their collective sense-making capacity. The COVID-19 "infodemic," January 6th Capitol attack, France's Gilets Jaunes protests, and Poland's hybrid threats from Russia and Belarus demonstrate how information manipulation directly threatens democratic stability. Yet responses reveal fundamental unresolved tensions between security imperatives and democratic values.

This research employs an integrated framework combining securitization theory, constructivist international relations, and democratic resilience studies to analyze how democratic states navigate protecting information integrity without sacrificing legitimacy. The Copenhagen School's securitization framework examines how information threats transition from technical issues to national security matters requiring extraordinary measures. Constructivism explains how strategic narratives shape threat perceptions and policy responses,

while resilience theory provides tools for understanding adaptive capacity under sustained pressure.

The case selection follows a “most different systems” design maximizing variation across key variables while controlling for democratic governance structures. The United States represents global hegemonic power with extensive strategic communication capabilities constrained by constitutional fragmentation and private sector autonomy. France exemplifies middle power strategic autonomy aspirations through centralized, state-directed cognitive security approaches. Poland illustrates small state adaptation within alliance frameworks while confronting immediate hybrid threats from authoritarian neighbors.

The methodology combines structured focused comparison with process tracing to identify causal mechanisms linking threat perception to institutional adaptation. Primary sources include official strategy documents, parliamentary testimony, declassified intelligence assessments, and elite interviews from 2022-2024. Secondary sources encompass academic analyses, think tank reports, and journalistic investigations providing independent policy effectiveness evaluation.

These cases enable systematic comparison across three dimensions: institutional response capacity (measured through doctrinal innovation, organizational adaptation, and resource allocation), societal resilience (assessed via trust metrics, civil society engagement, and crisis response effectiveness), and strategic adaptation (evaluated through technological integration, threat recognition, and international cooperation mechanisms).

The thesis traces strategic communication evolution through four distinct periods capturing technological transformation and shifting threat environments. The 1991-2001 period established post-Cold War information architecture characterized by Western narrative dominance and soft power emergence. The 2001-2011 decade witnessed information securitization following 9/11 and systematic information operations integration into military doctrine. The 2011-2020 period marked social media platforms’ transformation into contested strategic terrain for narrative control. The current 2020-2024 phase represents AI’s emergence as an information warfare force multiplier, fundamentally altering cognitive manipulation’s scale, precision, and attribution challenges.

This periodization reveals how technological disruption, geopolitical competition, and domestic pressures interact to create qualitatively different information environments requiring adaptive institutional responses. Contemporary information threats operate not merely through false content dissemination but through systematic exploitation of democratic societies' structural characteristics: openness to diverse viewpoints, reliance on public discourse for legitimacy, and individual expression rights protection.

The analysis reveals three distinct democratic response models reflecting different effectiveness-legitimacy balances. The American model emphasizes private sector leadership and technological solutions while maintaining strong constitutional constraints on government information activities. This provides significant innovation capacity and civil society resilience but creates coordination challenges and vulnerabilities to sophisticated state-sponsored operations.

The French model prioritizes state-directed strategic autonomy through centralized institutions and regulatory frameworks, enabling rapid crisis response and coherent policy implementation but raising democratic accountability concerns and potential authoritarian overreach. France's explicit cognitive warfare embrace represents the most militarized liberal democratic approach to information security.

The Polish model reflects frontline states' constraints and opportunities confronting immediate hybrid threats while building democratic institutions. Poland's emphasis on alliance integration and societal resilience through civil society engagement offers insights into how smaller democratic states can leverage multilateral frameworks while maintaining information governance autonomy.

This research advances several scholarly bodies while addressing pressing policy challenges. Theoretically, the analysis deepens understanding of securitization processes in the cognitive domain, where traditional domestic-international security boundaries blur. The developed framework provides tools for analyzing conditions under which democratic societies can successfully adapt to information warfare while preserving their fundamental character.

From a policy perspective, the research offers evidence-based insights into cognitive security governance trade-offs. The analysis suggests effective democratic responses require

balancing three competing imperatives: operational effectiveness in countering information threats, democratic legitimacy through accountability and transparency, and international credibility enabling alliance cooperation and norm development.

Part I establishes theoretical and historical foundations for comparative analysis. Part II presents detailed case studies analyzing each country's strategic communication institutions, vulnerability patterns, and adaptation strategies. Part III synthesizes comparative findings and develops forward-looking AI-era strategic communication analysis.

This research focuses specifically on democratic states confronting information threats while maintaining constitutional governance principles. The analysis does not comprehensively address authoritarian information control approaches, which operate under fundamentally different legitimacy constraints. The NATO allies emphasis limits generalizability to non-aligned democracies facing different technological and resource constraints.

The stakes extend beyond academic understanding to whether democratic societies can adapt to the information age without sacrificing defining openness and pluralism. As AI enables unprecedented cognitive manipulation at industrial scale, democratic institutions face pressures potentially exceeding their adaptive capacity. This comparative analysis provides sobering warnings about democratic vulnerabilities and grounds for cautious optimism about institutional innovation and societal resilience.

The research demonstrates that democratic information warfare responses cannot simply replicate authoritarian control models without undermining their own legitimacy. Instead, effective approaches must develop "democratic cognitive security", frameworks enhancing collective decision-making capacity while preserving epistemic pluralism essential for democratic legitimacy. Whether democratic societies possess necessary institutional creativity and political will for such innovation remains an open question largely determining twenty-first century democratic governance trajectories.

PART I - THEORETICAL, METHODOLOGICAL AND HISTORICAL FOUNDATIONS

This thesis employs a structured, focused comparison methodology[1] combined with process tracing to analyze how the United States, France, and Poland have adapted their strategic communication capabilities to address information threats from 1991 to 2024. The research design addresses both variation in outcomes (different institutional responses) and causal mechanisms (how threat perceptions translate into policy adaptation).

The selection of the United States, France, and Poland follows a "most different systems" design[2] that maximizes variation on key independent variables while controlling for the dependent variable (democratic governance structure). This selection strategy enables isolation of causal factors while maintaining analytical coherence.

The United States represents global hegemonic power with extensive strategic communication capabilities; France exemplifies middle power status with aspirations for strategic autonomy; Poland illustrates small state adaptation within alliance frameworks. Each state embodies distinct strategic traditions: American liberal institutionalism[3], French Gaullism emphasizing sovereignty[4], and Polish historical experience with foreign domination shaping threat perception[5]. Variation in civil-military relations, media systems, and administrative traditions affects strategic communication implementation. Different exposure levels to information warfare: the U.S. as global target, France as regional power balancing autonomy and alliance commitments, Poland as frontline state facing proximate Russian threats.

1. **Primary Sources:** Official strategy documents, military doctrine publications, parliamentary testimony, and declassified intelligence assessments provide authoritative insight into official thinking and institutional adaptation.

---

[1] George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005, pp. 67-72.
[2] Przeworski, Adam, and Henry Teune. *The Logic of Comparative Social Inquiry*. New York: Wiley, 1970, pp. 31-39.
[3] Ikenberry, G. John. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton: Princeton University Press, 2011.
[4] Vaïsse, Maurice. *La Grandeur: Politique étrangère du général de Gaulle, 1958-1969*. Paris: Fayard, 1998.
[5] Kuźniar, Roman. *Poland's Security Policy, 1989-2000*. Warsaw: Scholar Publishing House, 2001.

2. **Secondary Sources:** Academic analyses, think tank reports, and journalistic investigations offer independent evaluation of policy effectiveness and unintended consequences.
3. **Source Triangulation:** Multiple source types for each claim reduce potential bias from single-source reliance[6], while temporal comparison reveals policy evolution over time.
4. **Limitations:** Classification constraints limit access to operational details of strategic communication activities. Interview access with current officials was restricted due to security sensitivities, necessitating reliance on public statements and retrospective accounts.

Analytical Techniques [7]

1. **Process Tracing:** Identifies causal mechanisms linking threat perception to institutional adaptation by tracing decision-making sequences and policy rationales across time periods.
2. **Structured Comparison:** Systematic analysis across three dimensions (threat environment, institutional response capacity, and societal resilience metrics) enables controlled comparison while accounting for contextual variation.
3. **Temporal Analysis:** Four historical periods (1991-2001, 2001-2011, 2011-2020, 2020-2024) provide analytical structure while capturing both continuity and change in strategic communication evolution.

Potential Limitations and Biases [8]

1. **Selection Bias:** Focus on democratic states excludes authoritarian approaches to strategic communication, potentially limiting theoretical generalizability;

---

[6] Denzin, Norman K. *The Research Act: A Theoretical Introduction to Sociological Methods*. 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1989, pp. 234-247.

[7] Collier, David. "Understanding Process Tracing." *PS: Political Science & Politics* 44, no. 4 (2011): 823-830.; Mill, John Stuart. *A System of Logic, Ratiocinative and Inductive*. 8th ed. London: Longmans, Green, Reader, and Dyer, 1872, Book III, Chapter VIII.; Pierson, Paul. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2 (2000): 251-267.

[8] Geddes, Barbara. "How the Cases You Choose Affect the Answers You Get: Selection Bias in Comparative Politics." *Political Analysis* 2 (1990): 131-150.; King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press, 1994, pp. 128-138.; Lustick, Ian S. "History, Historiography, and Political Science: Multiple Historical Records and the Problem of Selection Bias." *American Political Science Review* 90, no. 3 (1996): 605-618.; Mearsheimer, John J., and Stephen M. Walt. "The Israel Lobby and U.S. Foreign Policy." *Middle East Policy* 13, no. 3 (2006): 29-87.

2. **Availability Bias:** Greater documentation of U.S. activities compared to French and Polish cases may skew analysis toward American experiences;
3. **Temporal Bias:** Emphasis on recent AI-related developments may underestimate continuity with historical practices;
4. **Analytical Bias:** Author's Western academic training may influence interpretation of non-Western strategic communication approaches.

CHAPTER 1: THEORETICAL FRAMEWORK

1.1 Reconceptualizing Security in the Post-Cold War Era

1.1.1. From traditional to non-traditional security

Security as a concept in International Relations has changed quite fundamentally since the Cold War ended. The traditional understanding, deeply rooted in realist thinking, primarily viewed security through the narrow lens of state survival in what realists see as an anarchic international system[9]. Stephen Walt captured this well when he defined security studies as dealing with "the phenomenon of war and the changing conditions that promote or prevent it"[10]. It is a definition that focuses almost exclusively on military threats to borders and state sovereignty. This state-centric approach made sense during the Cold War, emphasizing deterrence, defense, and managing competition between superpowers through military might[11].

But the post-1991 world quickly revealed just how limiting this narrow view had become. Transnational threats started emerging that did not fit neatly into the old categories: terrorism that crossed borders, organized crime networks, environmental problems that affected everyone, and these new cyber attacks that seemed to come from nowhere[12]. Barry Buzan, Ole Wæver, and Jaap

[9] Waltz, Kenneth N. "The Anarchic Structure of World Politics." In *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979, pp. 88-128.
[10] Walt, Stephen M. "The Renaissance of Security Studies." *International Studies Quarterly* 35, no. 2 (1991): 211-239, p. 212.
[11] Jervis, Robert. *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976.; Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.
[12] Keohane, Robert O., and Joseph S. Nye Jr. "Power and Interdependence in the Information Age." *Foreign Affairs* 77, no. 5 (1998): 81-94.; Rosenau, James N. *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton: Princeton University Press, 1990.

de Wilde made this point arguing that people could not keep limiting security to just military issues. Political, economic, societal, and environmental dimensions all matter now[13].

What is particularly interesting is how three interconnected domains have become so important in our information age: cybersecurity, information security, and cognitive security. These concepts are frequently conflated in the literature, which is understandable given their substantial conceptual overlap. But they are actually quite different challenges that need different approaches and responses[14].

Table 1.1: Comparison of Information-Age Security Domains

	Main Focus	***Types of Threats***	***How to Respond***	***Main Actors***
Cybersecurity	Protecting computer systems and networks	Malware, Hacking, System attacks	Technical defenses, Firewalls, Encryption	IT experts, Cyber units, Tech companies
Information Security	Protecting information quality and controlling narratives	False information, Propaganda, Influence campaigns	Fact-checking, Counter-messages, Platform rules	Media, intelligence services, Civil groups
Cognitive Security	Protecting mental resilience and clear thinking	Psychological manipulation, Confusion tactics, Trust destruction	Education, Critical thinking, Strong institutions	Schools, Psychologists, Democratic institutions

(Source: Author's elaboration)

Cybersecurity focuses on protecting digital infrastructure (the networks, systems, and data that run our modern world) from unauthorized access, disruption, or outright destruction[15]. Those 2007 cyber attacks on Estonia were a wake-up call, showing how a relatively small

[13] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998, pp. 7-42.
[14] Nye, Joseph S. Jr. "Cyber Power." *Belfer Center for Science and International Affairs*, Harvard Kennedy School, May 2010.
[15] Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014, pp. 15-32.

country could be brought to its knees through cyber means[16]. The Stuxnet operation against Iran's nuclear facilities in 2010 was perhaps even more eye-opening. It demonstrated how cyber threats could achieve what would traditionally require kinetic military force.

Information security addresses something different: the integrity, authenticity, and reliability of information itself within public discourse[17]. While cybersecurity is mostly technical, information security is more about the cognitive and social dimensions, about how information shapes what people believe, how they make decisions, and whether societies hold together. The 2016 U.S. election interference showed this perfectly: adversaries found ways to exploit information ecosystems and influence democratic processes without having to directly attack any technical infrastructure[18].

Cognitive security is probably the newest and definitely the most complex of these domains. It is about protecting the mental and epistemological resilience of both individuals and entire societies[19]. This gets at fundamental questions about how people process information, form beliefs, and maintain some shared understanding of what is actually real. Cognitive security threats work by exploiting psychological vulnerabilities, through targeted disinformation campaigns, deepfakes, algorithmic manipulation, all designed to erode trust in democratic institutions and tear apart social cohesion[20].

These three domains connect with two concepts that have become central to how to think about security today: societal resilience and communicative sovereignty.

Societal resilience refers to a society's ability to absorb, adapt to, and recover from information-based attacks while somehow maintaining democratic values and social cohesion[21]. Finland's comprehensive security model provides what might be the best example of this

[16] Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.
[17] Floridi, Luciano. "Information Ethics: On the Philosophical Foundation of Computer Ethics." *Ethics and Information Technology* 1, no. 1 (1999): 37-56.
[18] U.S. Senate Select Committee on Intelligence. *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure*. 116th Congress, 2020.
[19] Bjola, Corneliu, and Jen Wellings Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666.
[20] Roozenbeek, Jon, and Sander van der Linden. "Fake News Game Confers Psychological Resistance Against Online Misinformation." *Palgrave Communications* 5, no. 65 (2019): 1-10.
[21] Aldrich, Daniel P., and Michelle A. Meyer. "Social Capital and Community Resilience." *American Behavioral Scientist*59, no. 2 (2015): 254-269.

approach. They have managed to integrate government, civil society, and private sector responses to hybrid threats in ways that other countries are still trying to figure out[22].

Communicative sovereignty is about a state's capacity to maintain legitimate control over its information space against foreign interference while still preserving democratic discourse. France's 2018 anti-manipulation law (*loi contre la manipulation de l'information*) represents one attempt to make this work. It enables rapid judicial responses to disinformation during electoral periods, though it certainly raises some uncomfortable tensions between security imperatives and free expression[23].

The shift from traditional to non-traditional security really reflects much deeper changes in how power, conflict, and governance work in our globalized, information-saturated age[24]. Understanding these changes seems essential to analyze how contemporary democracies (including the United States, France, and Poland) are trying to protect their strategic communication networks against these hybrid threats that do not play by the old rules.

1.1.2. The Copenhagen School and Securitization Theory

The Copenhagen School's securitization theory probably offers the most influential framework for understanding how issues move from normal politics into the security domain[25]. Ole Wæver, Barry Buzan, and Jaap de Wilde developed this approach in the 1990s, and their core argument is that security is not really an objective condition but rather a social construction that happens through what they call "speech acts", performative utterances where someone declares an existential threat and justifies extraordinary measures to deal with it[26].

The securitization process involves three key parts: a securitizing actor (usually political leaders or institutions) who performs the speech act, a referent object (whatever is supposedly being threatened), and an audience that has to accept the security claim for securitization to

---

[22] Pynnöniemi, Katri, and András Rácz. "Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine." *Finnish Institute of International Affairs Report* 45 (2016).

[23] Assemblée Nationale. Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. *Journal Officiel de la République Française*, December 23, 2018.

[24] Keohane, Robert O., and Joseph S. Nye Jr. *Power and Interdependence*. 4th ed. Boston: Longman, 2011, pp. 220-244.

[25] Wæver, Ole. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz. New York: Columbia University Press, 1995, pp. 46-86.

[26] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998, pp. 23-26.

actually work. What is crucial here is that securitization lets actors move "beyond politics". They can bypass normal democratic procedures by invoking emergency response[27].

Securitization theory really helps illustrate how states transform what might seem like communication challenges into security imperatives. The European Union's response to Russian disinformation after the 2014 annexation of Crimea provides a textbook example of this process. European Council conclusions from June 2015 explicitly framed disinformation as undermining "European values and democratic principles" which justified creating the East StratCom Task Force[28]. This securitizing move enabled the EU to deploy resources and adopt measures (monitoring, debunking, strategic communications) that would have been much harder to justify politically as normal information policy.

The United States has gone through a similar securitization of information threats, though they have done it through different institutional mechanisms. The 2018 National Defense Authorization Act established Cyber Command's "information operations" mission, and the 2020 Joint Doctrine Note declared "information as a joint function"[29]. These documents frame information operations as threats to national security requiring military-level responses, essentially moving information warfare from the margins to the center of defense planning.

France's approach shows how securitization can happen at multiple levels simultaneously. At the EU level, France supported collective securitization through the East StratCom Task Force. Domestically, President Emmanuel Macron's 2017 declaration that "fake news" represented a threat to democracy enabled passage of restrictive information laws that had previously failed in parliament[30]. What is particularly telling is that these laws were first tested not against foreign disinformation but against the *Gilets Jaunes* (Yellow Vest) movement in 2018-2019, when authorities used anti-disinformation provisions to restrict social media content and monitor protest communications[31]. This demonstrates how securitization can expand well beyond its original justification.

---

[27] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998, pp. 23-26.

[28] European Council. "Council Conclusions on Countering Hybrid Threats." June 19, 2015. Brussels: European Council Press Office.

[29] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1631, 131 Stat. 1283 (2017).; U.S. Department of Defense. "Joint Doctrine Note 1-20: Information in the Joint Environment." April 24, 2020.

[30] Assemblée Nationale. "Proposition de loi relative à la lutte contre la manipulation de l'information." Session ordinaire 2017-2018, no. 799, March 21, 2018.

[31] Badouard, Romain. "The Yellow Vests and the Politicization of Digital Platforms." *French Politics* 18, no. 2 (2020): 238-251.

But securitization is not automatic or permanent. It requires audience acceptance and can face resistance or what scholars call "desecuritization" efforts[32]. In Poland, attempts by the Law and Justice (PiS) government to securitize media ownership through the 2021 "Lex TVN" law, framed as protecting information sovereignty against foreign manipulation, ran into significant domestic and international opposition and ultimately stalled in the Senate[33]. This case illustrates how securitization attempts can fail when audiences reject the threat construction or view the proposed measures as illegitimate.

The theory also raises some uncomfortable normative questions about the relationship between security and democracy. While securitization may enable rapid responses to genuine threats, it can also erode democratic accountability and civil liberties[34]. The challenge for democratic states appears to be developing what Thierry Balzacq calls "graduated securitization". There are the proportionate responses that address security concerns without completely abandoning normal political processes[35].

Securitization theory gives us essential analytical tools for understanding how information threats move from technical or political issues to matters of national security, shaping institutional responses and resource allocation in ways that have pretty profound implications for democratic governance.

1.2 Constructivism & the Power of Narrative in International Relations

Constructivism provides what might be called the metatheoretical foundation for understanding how strategic communication shapes international politics through the social construction of identities, interests, and threats[36]. Unlike rationalist approaches that treat state preferences as somehow given from the outside, constructivism emphasizes that "the manner in

[32] Hansen, Lene. "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School." *Millennium: Journal of International Studies* 29, no. 2 (2000): 285-306.
[33] Senate of Poland. "Ustawa o radiofonii i telewizji - Lex TVN." Proceedings of the Senate Committee on Culture and Media, September 11, 2021.
[34] Roe, Paul. "Securitization and Minority Rights: Conditions of Desecuritization." *Security Dialogue* 35, no. 3 (2004): 279-294.
[35] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq. London: Routledge, 2011, pp. 1-30.
[36] Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887-917.

which the material world shapes and is shaped by human action and interaction depends on dynamic normative and epistemic interpretations of the material world"[37].

Alexander Wendt's foundational insight that "anarchy is what states make of it" really demonstrates how international structures only acquire meaning through intersubjective understandings and shared practices[38]. From this perspective, security threats are not objective material facts but emerge through discursive processes that define what constitutes danger, identify relevant enemies, and legitimize specific response measures. Strategic narratives are coherent storylines providing meaning to past events and future possibilities and become central mechanisms through which political actors construct these security realities[39].

Strategic narratives seem to operate at three interconnected levels, as Alister Miskimmon, Ben O'Loughlin, and Laura Roselle have conceptualized: system narratives that explain the fundamental nature of the international order, identity narratives that construct national or group identities through historical memory and cultural symbols, and issue narratives that frame specific events or policies within broader meaning structures.[40]

The power of these narratives does not lie in their persuasive capacity but in what might be called constitutive effects. They create the social conditions that make specific policies possible or necessary[41]. The post-9/11 "War on Terror" narrative exemplifies this dynamic pretty well. By framing the attacks through civilizational discourse that positioned liberal democracy against radical extremism, this narrative enabled extraordinary measures including preemptive warfare, enhanced surveillance, and indefinite detention that would have been politically unacceptable under alternative framings[42].

Contemporary information warfare increasingly targets these narrative foundations, recognizing that identity and legitimacy have become primary sites of strategic competition. Russian information operations, as the RAND Corporation's "firehose of falsehood" study

---

[37] Adler, Emanuel. "Seizing the Middle Ground: Constructivism in World Politics." *European Journal of International Relations* 3, no. 3 (1997): 319-363, p. 322.
[38] Wendt, Alexander. "Anarchy is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 2 (1992): 391-425.
[39] Krebs, Ronald R., and Patrick Thaddeus Jackson. "Twisting Tongues and Twisting Arms: The Power of Political Rhetoric." *European Journal of International Relations* 13, no. 1 (2007): 35-66.
[40] Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. New York: Routledge, 2013, pp. 7-15.
[41] Searle, John R. *The Construction of Social Reality*. New York: Free Press, 1995, pp. 1-29.
[42] Jackson, Richard. *Writing the War on Terrorism: Language, Politics and Counter-terrorism*. Manchester: Manchester University Press, 2005.

analyzed[43], deliberately exploit identity cleavages within target societies. In Central and Eastern Europe, Russian strategic communications invoke historical traumas (i.e. Soviet occupation, Western betrayal) to reframe contemporary NATO and EU membership as neo-imperial projects threatening national sovereignty[44].

The 2019-2020 Russian disinformation campaign around Poland's Holocaust memory law illustrates this approach quite clearly. Russian media outlets amplified Polish-Jewish tensions by selectively highlighting controversial statements while promoting narratives that portrayed EU criticism as anti-Polish bias, exploiting existing identity conflicts to undermine transatlantic solidarity[45].

In the United States, malign actors have similarly weaponized identity narratives around race, politics, and cultural values. The 2016 Internet Research Agency operations demonstrated surprisingly sophisticated understanding of American identity cleavages, creating both "Black Lives Matter" and "Blue Lives Matter" content to amplify social divisions[46]. These campaigns succeeded not by creating new divisions but by exploiting existing fault lines in American identity narratives.

This targeting of identity reveals what appears to be a crucial shift in the nature of conflict: information warfare increasingly aims not at persuasion but at fragmentation eroding shared epistemic foundations that enable democratic deliberation. As Lawrence Freedman argues in his analysis of strategic communications, the goal is often not winning arguments but "creating enough confusion and doubt to undermine the confidence required for decisive action"[47].

Constructivism clarifies how communication infrastructures (e.g. social media platforms, algorithmic content curation, news ecosystems) function as contested terrains where political realities are continuously produced and challenged[48]. Control over these narrative spaces increasingly translates into strategic advantage, as China's efforts to promote alternative system

---

[43] Paul, Christopher, and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model." *RAND Perspective*PE-198-OSD (2016).
[44] Grigas, Agnia. *Beyond Crimea: The New Russian Empire*. New Haven: Yale University Press, 2016, pp. 178-203.
[45] EUvsDisinfo. "The Kremlin this Week: Let's hate Poland!" January 23, 2020.
[46] U.S. Senate Select Committee on Intelligence. *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media*. 116th Congress, 2020.
[47] Freedman, Lawrence. "The Transformation of Strategic Affairs." *Adelphi Paper* 379 (2006): 7-100, p. 45.
[48] van Dijck, José. *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press, 2013, pp. 145-171.

narratives through media investments, academic partnerships, and digital infrastructure projects under the Belt and Road Initiative seem to demonstrate[49].

For democratic societies, this constructivist understanding highlights both vulnerabilities and opportunities. While openness makes democracies susceptible to narrative manipulation, the same pluralistic discourse that creates vulnerability may also provide resources for resilience through counter-narratives, fact-checking, and public debate. The challenge lies in maintaining these democratic strengths while developing defensive capabilities against systematic narrative attacks[50].

This analytical framework positions strategic communication not as some peripheral support function but as central to contemporary security practice, requiring sophisticated understanding of how narratives construct political possibilities and constrain strategic choices in our increasingly interconnected world.

1.3 The Evolution of Information Warfare Theory

The conceptual landscape of information warfare has undergone what can only be described as dramatic transformation, evolving from a peripheral military concern to a primary domain of strategic competition[51]. This evolution reflects broader changes in how information technologies mediate political power, social cohesion, and interstate conflict. Understanding this trajectory requires careful attention to definitional precision, doctrinal innovation, and the integration of emerging technologies into strategic frameworks[52].

1.3.1 Defining the Threat Landscape

Contemporary information warfare operates across multiple dimensions that really need analytical disaggregation. Building on Claire Wardle and Hossein Derakhshan's foundational

[49] Shambaugh, David. "China's Soft-Power Push: The Search for Respect." *Foreign Affairs* 94, no. 4 (2015): 99-107.
[50] Rosen, Armin. "How Democracies Can Win the Information War." *The Atlantic*, March 15, 2019.
[51] Arquilla, John, and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation, 1997.
[52] Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007, pp. 1-25.

taxonomy, which has been refined by subsequent scholarship from places like the Reuters Institute and the Computational Propaganda Research Project, three primary categories of information threats have emerged[53]:

1. **Misinformation** refers to false or misleading content shared without malicious intent. This includes honest mistakes, misinterpretation of events, or people inadvertently spreading unverified information. While not deliberately harmful, misinformation can still create operational challenges during crises when rapid, accurate information sharing becomes critical for public safety and coordinated response[54].
2. **Disinformation** encompasses deliberately false information created and disseminated with intent to deceive, manipulate, or cause harm. This represents the core of adversarial information operations, involving systematic campaigns designed to influence political processes, undermine institutional trust, or destabilize social cohesion. The 2020 "Plandemic" conspiracy theory exemplifies sophisticated disinformation. It combined fabricated expert testimony with selective data manipulation to undermine public health responses[55].
3. **Malinformation** involves authentic information weaponized to cause harm through strategic timing, contextualization, or amplification. This includes leaked materials, private communications, or embarrassing but truthful content deployed to damage reputations or institutions. The 2017 Macron campaign email leaks demonstrate malinformation tactics, authentic materials released strategically before the French presidential election to maximize political damage[56].

These categories intersect with what NATO's StratCom Centre of Excellence terms "cognitive warfare". These operations target human cognition to influence perception, decision-making, and behavior[57]. Unlike traditional propaganda that seeks to persuade, cognitive

[53] Wardle, Claire, and Hossein Derakhshan. "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making." *Council of Europe Report* DGI(2017)09 (2017).
[54] *Ibid.*
[55] Wilson, Jameson, and Sarah Starbird. "Cross-Platform Information Operations and the 'Plandemic' Conspiracy Theory." *Harvard Kennedy School Misinformation Review* 2, no. 1 (2021): 1-18.
[56] Prentoulis, Marina, and Lasse Thomassen. "The Macron Moment and the Future of Europe." *Constellations* 25, no. 3 (2018): 437-451.
[57] Backes, Swen, and Alek Swab. "Cognitive Warfare: The Future of Cognitive Dominance." *NATO Strategic Communications Centre of Excellence* (2019).

warfare aims to confuse, paralyze, or fragment target audiences by undermining their capacity for rational deliberation[58].

1.3.2 Doctrinal and Conceptual Approaches

State responses to information warfare reflect different strategic cultures, threat perceptions, and institutional capabilities, resulting in what appear to be quite divergent doctrinal frameworks[59].

The U.S. Department of Defense's 2020 Joint Doctrine Note represents what might be called a paradigmatic shift, formally recognizing "information as a joint function" alongside traditional warfighting domains[60]. This elevation signals that information operations are no longer auxiliary to kinetic operations but co-equal components of military strategy across all phases of conflict.

General Paul Nakasone, former Director of NSA and Commander of U.S. Cyber Command, articulated this evolution in Congressional testimony: "We must compete in the information environment [because] our adversaries have weaponized information to undermine democratic institutions and weaken alliance cohesion"[61]. This competitive framing justifies "persistent engagement" strategies that proactively contest adversarial narratives rather than merely defending against attacks[62].

NATO's Strategic Communications (StratCom) doctrine, codified in the 2017 Joint Doctrine for Strategic Communications (AJP-10), emphasizes synchronized messaging across diplomatic, military, and informational instruments. NATO defines StratCom as "the coordinated

---

[58] Backes, Swen, and Alek Swab. "Cognitive Warfare: The Future of Cognitive Dominance." *NATO Strategic Communications Centre of Excellence* (2019).

[59] Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge, 2011, pp. 45-67.

[60] U.S. Joint Chiefs of Staff. "Joint Doctrine Note 1-20: Information in the Joint Environment." April 24, 2020.

[61] House Armed Services Committee. "Statement of General Paul M. Nakasone, Director, National Security Agency, Commander, U.S. Cyber Command." Hearing on Fiscal Year 2022 National Defense Authorization Budget, April 15, 2021.

[62] U.S. Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command." April 2018.

and appropriate use of NATO communications activities and capabilities [...] in support of Alliance policies, operations and activities, and in order to advance NATO's aims"[63].

The establishment of NATO's Strategic Communications Centre of Excellence in Riga back in 2014 institutionalized this approach, conducting research, training, and operational support for member states[64]. The Centre's annual conferences have become focal points for developing alliance responses to hybrid threats, emphasizing both defensive measures (resilience-building) and what they call offensive capabilities (strategic messaging)[65].

France has pioneered what they call "cognitive warfare" (*guerre cognitive*), formally incorporated into the 2019 Military Programming Law. This framework explicitly recognizes the cognitive battlefield as a primary theater of operations where adversaries exploit informational and cultural asymmetries to manipulate public opinion and fracture social trust[66].

French military doctrine, as articulated in the 2020 Strategic Review, emphasizes "information sovereignty" (*souveraineté informationnelle*), the capacity to maintain autonomous control over national information spaces[67]. This concept seems to underlie France's resistance to American technology dominance and support for European digital sovereignty initiatives, including GDPR implementation and platform regulation.

The French approach integrates military and civilian capabilities through the National Intelligence Coordinator (*Coordonnateur national du renseignement)*, which synchronizes responses across defense, interior, and foreign affairs ministries. This whole-of-government model reflects French administrative culture while addressing the hybrid nature of contemporary information threats[68].

[63] NATO. "AJP-10: Allied Joint Doctrine for Strategic Communications." December 2017.
[64] NATO Strategic Communications Centre of Excellence. "About NATO StratCom COE." Accessed June 2025.
[65] NATO StratCom COE. "Annual Report 2021." Riga: NATO StratCom COE, 2022.
[66] Assemblée Nationale. Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025. *Journal Officiel de la République Française*, July 14, 2018.; Henrotin, Joseph. "La guerre cognitive: un nouveau champ de bataille?" *Défense & Sécurité Internationale* 154 (2020): 52-57.
[67] Ministère des Armées. "Revue stratégique de défense et de sécurité nationale." Paris: Direction générale des relations internationales et de la stratégie, 2020.
[68] Irondelle, Bastien. "The French Approach to Strategic Communications." In *Strategic Communications in International Relations*, edited by Corneliu Bjola and Marcus Holmes. London: Routledge, 2015, pp. 134-148.

1.3.3 PSYOPS, IO, and Strategic Communication

The evolution from psychological operations (PSYOPS) through information operations (IO) to strategic communication (StratCom) reflects expanding conceptualization of information's role in conflict and governance[69].

Psychological Operations (PSYOPS) traditionally focused on influencing adversary decision-makers through targeted messaging, often tactical and campaign-specific[70]. Classic PSYOPS included things like leaflet drops, radio broadcasts, and deception operations designed to demoralize enemy forces or civilian populations. The Gulf War's "Highway of Death" broadcasts exemplified this approach, tactical messaging designed to encourage Iraqi troop surrender[71].

Information Operations (IO) expanded beyond PSYOPS to encompass a broader range of information-related military activities, including electronic warfare, computer network operations, and operational security[72]. The U.S. military's definition of IO as actions designed "to affect information and information systems while defending one's own information and information systems" reflects this more integrated approach[73].

Strategic Communication (StratCom) represents perhaps the most comprehensive framework, extending beyond military contexts to encompass whole-of-government approaches that align words, images, and actions to achieve policy objectives. StratCom integrates public diplomacy, military public affairs, and international broadcasting into coherent narrative strategies designed to shape long-term perceptions rather than achieve immediate tactical effects[74].

The COVID-19 pandemic illustrated this continuum in practice quite well. During the 2020-2021 crisis, governments deployed StratCom not merely to inform but to shape public

---

[69] Goldstein, Frank L., and Benjamin F. Findley Jr., eds. *Psychological Operations: Principles and Case Studies*. Maxwell Air Force Base: Air University Press, 1996, pp. 1-25.
[70] Linebarger, Paul M. A. *Psychological Warfare*. 2nd ed. New York: Arno Press, 1972, pp. 12-34.
[71] Atkinson, Rick. *Crusade: The Untold Story of the Persian Gulf War*. Boston: Houghton Mifflin, 1993, pp. 412-425.
[72] Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, eds. *Cyberwar: Security, Strategy and Conflict in the Information Age*. Fairfax: AFCEA International Press, 1996, pp. 87-104.
[73] U.S. Joint Chiefs of Staff. "Joint Publication 3-13: Information Operations." November 20, 2014.
[74] Hallahan, Kirk, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič, and Krishnamurthy Sriramesh. "Defining Strategic Communication." *International Journal of Strategic Communication* 1, no. 1 (2007): 3-35.

behavior, maintain social cohesion, and counter conspiracy theories[75]. The U.S. Surgeon General's declaration of a "health misinformation infodemic" exemplified how public health communication increasingly resembles wartime strategic messaging, complete with adversary identification (conspiracy theorists) and mobilization rhetoric[76].

This operational evolution reflects what appears to be a fundamental shift: information warfare now extends beyond military-to-military or state-to-state competition to encompass systematic attempts to influence entire societies through their communication ecosystems[77]. This transformation requires new theoretical frameworks capable of analyzing information not merely as a tool of statecraft but as a domain of conflict itself.

1.4 Hybrid Threats & Societal Resilience

Hybrid threats may represent the most complex and widespread challenge facing contemporary security today. They are characterized by the coordinated use of conventional and unconventional instruments that stay just below the threshold of traditional warfare[78]. What makes these campaigns particularly dangerous is their strategic weaponization of information not merely to inform or persuade, but to systematically chip away at social cohesion, institutional trust, and the capacity for democratic decision-making[79]. This section examines theoretical frameworks for understanding hybrid warfare, explores artificial intelligence as a force multiplier, and considers societal resilience as an emerging paradigm for democratic defense.

---

[75] Reuter, Ora John, and David Szakonyi. "Elite Cues and Citizen Compliance with Public Health Measures." *Journal of Politics* 83, no. 4 (2021): 1562-1577.
[76] Murthy, Vivek H. "Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building a Healthy Information Environment." U.S. Department of Health and Human Services, 2021.
[77] Mazarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews. "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment." *RAND Research Report* RR-2714-OSD (2019).
[78] Cullen, Patrick J., and Erik Reichborn-Kjennerud. "Understanding Hybrid Warfare." *MCDC Countering Hybrid Warfare Project* (2017): 1-24.
[79] Wigell, Mikael. "Democratic Deterrence: How to Dissuade Hybrid Interference." *Washington Quarterly* 44, no. 1 (2021): 49-67.

1.4.1 Understanding Hybrid Warfare

Hybrid warfare, as both NATO and EU frameworks have attempted to define it, involves "the synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects". This definition highlights three critical characteristics: synchronisation across multiple domains, tailored targeting of specific vulnerabilities, and synergistic effects that appear to exceed the sum of individual components[80].

Frank Hoffman's foundational analysis identified hybrid threats as blending "lethality of state conflict with the fanatical and protracted fervor of irregular warfare"[81]. However, subsequent research has expanded this framework well beyond military dimensions. Contemporary hybrid campaigns weave together diplomatic pressure, economic coercion, cyber attacks, disinformation, and support for proxy actors in ways that create strategic effects without crossing formal thresholds for military response[82].

The concept of "reflexive control" developed in Soviet military theory and refined in contemporary Russian strategic thinking offers useful insight into hybrid warfare's informational dimensions. Vladimir Lefebvre originally formulated it as "conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator"[83]. Today's applications extend this concept to entire societies, where disinformation campaigns do not aim at direct persuasion but rather at shaping the informational environment to provoke self-defeating responses[84].

The 2014-2016 Russian hybrid campaign against Ukraine demonstrates this integrated approach quite clearly. Beyond the military intervention in Crimea and eastern Ukraine, the campaign included economic pressure through energy pricing, cyber attacks on critical infrastructure, diplomatic isolation efforts, and sophisticated information operations targeting

---

[80] European Centre of Excellence for Countering Hybrid Threats. "Hybrid Threats as a Phenomenon." Helsinki: Hybrid CoE, 2019.
[81] Hoffman, Frank G. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington: Potomac Institute for Policy Studies, 2007, p. 8.
[82] Renz, Bettina. "Russia and 'Hybrid Warfare': Going Beyond the Label." *Aleksanteri Papers* 1 (2016): 1-52.
[83] Lefebvre, Vladimir A. "Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process." *Science Applications International Corporation* (1984), p. 3.
[84] Jonsson, Oscar, and Robert Seely. "Russian Full-Spectrum Conflict: An Appraisal After Ukraine." *Journal of Slavic Military Studies* 28, no. 1 (2015): 1-22.

both Ukrainian and international audiences[85]. The information component seems to have deliberately exploited existing societal divisions (linguistic, regional, historical) while promoting narratives of Ukrainian state illegitimacy and Western manipulation[86].

Disinformation functions as what Lawrence Freedman calls "the most cost-effective weapon" in hybrid arsenals[87]. This is likely because it exploits democratic vulnerabilities (openness, pluralism, free expression) while remaining difficult to attribute or counter without potentially undermining the very democratic values it attacks. The asymmetric nature of this challenge is stark: authoritarian states can flood democratic information spaces with falsehoods while maintaining strict control over their own domestic narratives[88].

1.4.2 AI as a Force Multiplier

Artificial intelligence has fundamentally altered the scale, precision, and effectiveness of information warfare[89]. What were previously labor-intensive, imprecise influence operations have been transformed into automated, targeted, and adaptive campaigns. AI technologies enable three critical capabilities that appear to exponentially increase disinformation impact: automation of content generation and distribution, personalization based on individual psychological profiles, and real-time adaptation to audience responses and countermeasures[90].

The emergence of sophisticated synthetic media including deepfake videos, AI-generated text, and voice synthesis poses unprecedented challenges to what might be called epistemological security. The 2019 deployment of deepfake technology in Gabonese political

[85] Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. "Lessons from Russia's Operations in Crimea and Eastern Ukraine." *RAND Research Report* RR-1498-A (2017).
[86] Darczewska, Jolanta. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study." *Centre for Eastern Studies* 42 (2014): 1-64..
[87] Freedman, Lawrence. "Information, Disinformation and Political Warfare." In *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, Brian Mazanec, and Brandon Valeriano. London: Routledge, 2019, pp. 15-32.
[88] King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111, no. 3 (2017): 484-501.
[89] Goldfarb, Avi, and Jon Lindsay. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46, no. 3 (2022): 7-50.
[90] Bateman, Jon. "U.S. Foreign Policy and the AI Revolution." *Carnegie Endowment for International Peace* (2022): 45-67.

manipulation and the 2020 emergence of GPT-3 generated propaganda demonstrate how AI can fabricate convincing content across multiple media formats[91].

Perhaps more concerning than individual deepfakes is what researchers term "the liar's dividend", the broader epistemic uncertainty created by awareness that any content might be artificial. This uncertainty appears to benefit disinformation actors by undermining confidence in authentic evidence, enabling political actors to dismiss inconvenient truths as "fake news" or potential deepfakes[92].

Social media algorithms designed to maximize engagement inadvertently optimize for emotional arousal, controversy, and confirmation bias[93]. These characteristics align remarkably well with disinformation's psychological impact strategies. The 2018 Congressional testimony by Facebook's internal data science teams revealed that their algorithms preferentially amplified divisive content because it generated higher user engagement[94].

AI-enhanced micro-targeting capabilities enable disinformation campaigns to deliver specifically crafted messages to psychologically vulnerable audiences based on detailed behavioral profiles[95]. The Cambridge Analytica scandal demonstrated how these capabilities could be weaponized for political manipulation, but subsequent research suggests far more sophisticated targeting may now be possible using publicly available data and machine learning algorithms[96].

However, AI also offers defensive capabilities for detecting and countering disinformation[97]. Companies like Microsoft and Google have developed AI systems capable of identifying deepfakes, tracking coordination networks, and flagging suspicious content patterns.

---

[91] Paris, Britt, and Joan Donovan. "Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence." *Data & Society Research Institute* (2019): 12-18.

[92] Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753-1820, pp. 1792-1798.

[93] Tufekci, Zeynep. "Algorithmic Amplification of Politics on Twitter." *Proceedings of the National Academy of Sciences*119, no. 1 (2022).

[94] House Committee on Energy and Commerce. "Facebook: Transparency and Use of Consumer Data." Hearing, April 11, 2018. 115th Congress, 2nd Session.

[95] Susser, Daniel, Beate Roessler, and Helen Nissenbaum. "Technology, Autonomy, and Manipulation." *Internet Policy Review* 8, no. 2 (2019): 1-22.

[96] Kaiser, Brittany. *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. New York: HarperCollins, 2019, pp. 145-167.

[97] Stamos, Alex. "Information Operations and Facebook." *Center for International Security and Cooperation*, Stanford University (2019): 23-35.

The Partnership on AI's initiative on synthetic media detection represents collaborative efforts to develop technical solutions[98].

Yet the offensive-defensive balance remains heavily skewed toward attackers. Creating convincing deepfakes requires significantly fewer resources than developing reliable detection systems, and adversaries can continuously adapt their techniques to evade detection algorithms[99]. This asymmetry particularly disadvantages smaller states with limited technical capabilities.

1.4.3 Resilience as National Strategy

The complexity and persistence of hybrid threats have prompted many democracies to shift from reactive defense to proactive resilience-building as their primary strategic approach. Societal resilience, in this context, encompasses not merely the capacity to recover from attacks but the ability to maintain democratic functions, social cohesion, and institutional legitimacy while under sustained pressure[100].

Finland's "comprehensive security" framework represents perhaps the most developed model of societal resilience against hybrid threats[101]. Originally developed during the Cold War to manage Soviet pressure, this approach has been updated for contemporary information warfare challenges. The model integrates four key components:

1. **Whole-of-society preparation:** All sectors (i.e. government, private industry, civil society, and individual citizens) receive training in recognizing and responding to hybrid threats. Finland's National Defence Courses, attended by over 60,000 citizens since 1961, now include modules on media literacy and information warfare[102].

[98] Partnership on AI. "Framework for AI and Media Integrity." Partnership on AI (2020): 1-25.
[99] Scharre, Paul. "Deepfakes and the Coming AI Dystopia." *War on the Rocks*, February 15, 2019.
[100] Boin, Arjen, and Michel J. G. van Eeten. "The Resilient Organization." *Public Administration* 91, no. 2 (2013): 429-445.
[101] Government of Finland. "Security Strategy for Society: Government Resolution." Helsinki: Security Committee, 2017.
[102] Finnish Government. "Finland's Comprehensive Security Model." Prime Minister's Office Publications 2021/4 (2021): 25-32.

2. **Institutional redundancy:** Critical functions are distributed across multiple institutions to prevent single points of failure. Finland maintains strong public broadcasting (YLE) alongside diverse private media, ensuring information pluralism even under attack[103].
3. **Rapid response capabilities:** The National Emergency Supply Agency coordinates government, private sector, and civil society responses to crises, enabling quick correction of false information and coordinated messaging during emergencies[104].
4. **Social trust and cohesion:** High levels of institutional trust (Finland consistently ranks among the world's most trusted societies in international surveys) may provide resilience against disinformation designed to exploit cynicism and polarization[105].

The effectiveness of Finland's approach was demonstrated during the 2016 "Little Green Men" disinformation campaign, when Russian media falsely claimed NATO forces had raped Finnish women. Finnish authorities, media, and civil society quickly debunked the claims while maintaining calm public discourse, preventing the polarization seen in other targeted countries[106].

However, the Finnish model's applicability to more polarized democracies remains questionable[107]. Societies with high political polarization, low institutional trust, and fragmented media ecosystems face greater challenges in building resilience. The United States' struggle with COVID-19 misinformation illustrates this dynamic quite well. Even accurate government health guidance faced rejection from significant population segments due to political polarization and institutional distrust[108].

Research by the Reuters Institute demonstrates strong correlations between political polarization and susceptibility to misinformation, suggesting that resilience-building may require

---

[103] Wigell, Mikael, Sören Scholvin, and Minna Aaltola, eds. *Geo-economics and Power Politics in the 21st Century: The Revival of Economic Statecraft*. London: Routledge, 2018, pp. 134-149.
[104] Finnish Government. "Finland's Comprehensive Security Model." Prime Minister's Office Publications 2021/4 (2021): *pp. 35-38.*
[105] Helliwell, John F., Richard Layard, Jeffrey D. Sachs, and Jan Emmanuel De Neve, eds. *World Happiness Report 2021*. New York: Sustainable Development Solutions Network, 2021, pp. 45-52.
[106] European Centre of Excellence for Countering Hybrid Threats. "The Finnish Model for Countering Hybrid Threats." Helsinki: Hybrid CoE, 2018.
[107] Norris, Pippa. *Democratic Deficit: Critical Citizens Revisited*. Cambridge: Cambridge University Press, 2011, pp. 215-238.
[108] Goldberg, Matthew H., et al. "Social Norms Motivate COVID-19 Preventive Behaviors." *PsyArXiv* (2020): 1-25.

addressing underlying social divisions rather than merely improving technical countermeasures[109].

The resilience paradigm therefore represents both an opportunity and a challenge for contemporary democracies. It offers a comprehensive approach to hybrid threats but requires social conditions (trust, cohesion, institutional legitimacy) that hybrid warfare specifically targets for erosion[110]. Successfully implementing resilience strategies may therefore require fundamental investments in democratic renewal alongside technical defensive capabilities.

1.5 Analytical Framework of the Thesis

This thesis develops an integrated analytical framework that combines constructivist, securitization, and strategic communication theories to examine how democratic states adapt to hybrid information threats in the AI era[111]. The framework allows for systematic comparison of national responses while accounting for the dynamic interactions between technological change, threat perception, and institutional adaptation.

1.5.1 Synthesis of Theoretical Strands

The analytical framework operates across three interconnected theoretical levels that capture different dimensions of contemporary information warfare[112]:

1. **Ideational-Normative Level (Constructivism)**

Constructivism provides the foundational layer for understanding how states interpret their strategic environments and construct appropriate responses. This level examines how national identities, historical experiences, and strategic cultures shape threat perception and

[109] Newman, Nic, Richard Fletcher, Anne Schulz, Simge Andi, Craig Robertson, and Rasmus Kleis Nielsen. "Reuters Institute Digital News Report 2021." Oxford: Reuters Institute for the Study of Journalism, 2021.
[110] Aldrich, Daniel P., and Michelle A. Meyer. "Social Capital and Community Resilience." *American Behavioral Scientist* 59, no. 2 (2015): 254-269.
[111] George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005, pp. 233-262.
[112] Guzzini, Stefano. "A Reconstruction of Constructivism in International Relations." *European Journal of International Relations* 6, no. 2 (2000): 147-182.

policy choices[113]. It focuses particularly on how states narrate their security challenges and how these narratives may influence institutional development and resource allocation[114].

Key analytical questions include: How do different national identities and strategic cultures influence the interpretation of information threats? What role might historical experiences (e.g., authoritarianism, foreign occupation, democratic transition) play in shaping contemporary responses? How do states construct and project strategic narratives to maintain legitimacy during information conflicts?

2. **Discursive-Political Level (Securitization Theory)**

Securitization theory enables analysis of how information threats transition from technical or political issues to matters of national security[115]. This level examines speech acts, audience acceptance, and the political processes through which extraordinary measures become legitimized. It also addresses the normative tensions that appear between security imperatives and democratic values[116].

Key analytical questions include: Which actors successfully securitize information threats and through what mechanisms? How do different democratic institutions (parliaments, courts, media) respond to securitization attempts? What are the consequences intended and unintended of securitizing information challenges?[117]

3. **Operational-Technological Level (Strategic Communication Doctrine)**

This level examines how theoretical frameworks translate into practical capabilities, institutional structures, and operational responses. It analyzes the integration of AI technologies, platform regulation, international cooperation, and civil society engagement in national strategic communication strategies[118].

---

[113] Katzenstein, Peter J., ed. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996, pp. 1-32.
[114] Hopf, Ted. "The Promise of Constructivism in International Relations Theory." *International Security* 23, no. 1 (1998): 171-200.
[115] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998, pp. 23-47.
[116] Roe, Paul. "Securitization and Minority Rights: Conditions of Desecuritization." *Security Dialogue* 35, no. 3 (2004): 279-294.
[117] McDonald, Matt. "Securitization and the Construction of Security." *European Journal of International Relations* 14, no. 4 (2008): 563-587.
[118] Cornish, Paul, Julian Lindley-French, and Claire Yorke. "Strategic Communications and National Strategy." *Chatham House Briefing Paper* (2011): 1-12.

Key analytical questions include: How do states organize and coordinate their strategic communication capabilities? What role do AI technologies play in both offensive and defensive information operations? How effective are different institutional models in responding to rapid technological change?

These levels interact through feedback loops: securitization processes influence operational capabilities, which shape threat perceptions, which inform narrative construction, completing the analytical cycle[119].

1.5.2 Operationalizing Concepts for Case Studies

To enable systematic empirical comparison, the framework operationalizes key concepts through observable indicators organized around two primary dimensions: institutional response capacity and societal resilience metrics[120].

Institutional Response Capacity Indicators

Doctrinal Innovation: Analysis of official strategic documents incorporating information warfare, hybrid threats, or cognitive security concepts. This includes national security strategies, defense white papers, cybersecurity frameworks, and AI governance policies[121]. Temporal analysis tracks doctrinal evolution and cross-national diffusion of concepts.

Organizational Adaptation: Examination of institutional development including establishment or expansion of strategic communication units, cyber commands, hybrid threat centers, and AI oversight bodies[122]. This includes budget allocations, personnel assignments, and inter-agency coordination mechanisms.

Legal-Regulatory Frameworks: Assessment of legislative and regulatory responses to information threats, including platform regulation, disinformation laws, election security

---

[119] Checkel, Jeffrey T. "The Constructivist Turn in International Relations Theory." *World Politics* 50, no. 2 (1998): 324-348.

[120] King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press, 1994, pp. 109-149.

[121] Bennett, Andrew, and Jeffrey T. Checkel, eds. *Process Tracing: From Metaphor to Analytic Tool*. Cambridge: Cambridge University Press, 2015, pp. 3-37.

[122] March, James G., and Johan P. Olsen. "The New Institutionalism: Organizational Factors in Political Life." *American Political Science Review* 78, no. 3 (1984): 734-749.

measures, and AI governance frameworks[123]. Analysis includes implementation effectiveness and democratic oversight mechanisms.

International Cooperation: Evaluation of participation in multilateral frameworks (NATO StratCom, EU East StratCom, bilateral agreements) and contribution to alliance capabilities[124]. This includes burden-sharing analysis and assessment of interoperability with partner nations.

Societal Resilience Metrics

Threat Recognition: Analysis of elite and public discourse regarding information threats through parliamentary debates, media coverage, and public opinion surveys[125]. This includes tracking of threat salience and framing consistency across different audiences.

Educational Investment: Assessment of media literacy programs, critical thinking curricula, and digital citizenship initiatives across educational systems and civil society organizations[126]. This includes budget analysis and outcome evaluation where available.

Institutional Trust: Longitudinal analysis of public confidence in democratic institutions, media organizations, and information sources using established survey instruments (Eurobarometer, World Values Survey, national polling)[127]. Cross-national comparison may identify vulnerability patterns and resilience factors.

Crisis Response Effectiveness: Case-based evaluation of response speed, coordination quality, and message consistency during information crises (elections under attack, pandemic misinformation, international incidents)[128]. This includes process tracing of decision-making and outcome assessment.

---

[123] Baldwin, David A., ed. *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press, 1993, pp. 3-25.

[124] Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984, pp. 85-109.

[125] Entman, Robert M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43, no. 4 (1993): 51-58.

[126] Potter, W. James. *Media Literacy*. 8th ed. Thousand Oaks: SAGE Publications, 2016, pp. 45-67.

[127] Inglehart, Ronald, et al. "World Values Survey: Round Seven–Country-Pooled Datafile Version 4.0." Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat, 2022.

[128] George and Bennett, *Case Studies and Theory Development*, pp. 205-232.

The framework enables structured comparison through three analytical dimensions[129]:

1. **Threat Environment:** Similarity/difference in information threats faced (Russian disinformation, domestic polarization, technological vulnerability);
2. **Institutional Context:** Variations in political systems, administrative traditions, and civil society structures that influence response capacity;
3. **Strategic Choices:** Different approaches to balancing security imperatives with democratic values, offensive versus defensive capabilities, and national versus multilateral response.

1.5.3 Conceptual Model

The thesis proposes a dynamic triadic model capturing the interactive relationships between narrative environment, technological infrastructure, and state response mechanisms[130]:

1. **Narrative Environment:** The contested informational space where identities, legitimacy, and policy preferences are continuously constructed and challenged. This includes both state strategic narratives and adversarial counter-narratives, domestic political discourse, and international diplomatic messaging[131].
2. **Technological Infrastructure:** The socio-technical systems through which information flows and is processed, including AI algorithms, social media platforms, traditional media organizations, and emerging technologies. These systems function as both enablers of democratic communication and potential vulnerabilities for hostile exploitation[132].
3. **State Response Mechanisms:** The institutional, legal, and operational adaptations states develop to defend, shape, and contest narrative environments. This includes both defensive measures (resilience-building, countermessaging) and offensive capabilities (strategic influence, information operations)[133].

---

[129] Lijphart, Arend. "Comparative Politics and the Comparative Method." *American Political Science Review* 65, no. 3 (1971): 682-693.; Putnam, Robert D. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427-460.
[130] Easton, David. *A Systems Analysis of Political Life*. New York: John Wiley & Sons, 1965, pp. 21-33.
[131] Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. New York: Routledge, 2013, pp. 5-15.
[132] Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121-136.
[133] North, Douglass C. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990, pp. 3-35.

Interactive Dynamics

Threat-Response Feedback: Successful disinformation campaigns that exploit systemic vulnerabilities trigger institutional innovation and policy adaptation. The Russian interference in the 2016 U.S. election, for example, prompted creation of new government units, legislative initiatives, and private sector cooperation mechanisms[134].

Securitization-Legitimacy Tension: Securitization processes that justify extraordinary measures risk undermining the democratic values they aim to protect. Over-securitization can erode civil liberties and free expression, while under-securitization may leave societies vulnerable to manipulation[135].

Technology-Strategy Co-evolution: Technological developments continuously reshape both threat landscapes and response capabilities, requiring adaptive institutional structures and strategic frameworks. The emergence of large language models (GPT-3/4) demonstrates how rapid technological change can outpace existing regulatory and defensive frameworks[136].

This model enables dynamic analysis that captures how strategic communication, technological change, and democratic governance interact in contemporary security environments. It provides a scalable framework for assessing not merely current capabilities but adaptive capacity that is the ability to respond effectively to emerging threats while maintaining democratic legitimacy[137].

The framework positions strategic communication as neither purely technical nor purely political but as a complex socio-technical domain requiring sophisticated theoretical tools and empirical analysis. It provides the foundation for examining how different democratic states navigate the fundamental challenges of protecting open societies in an era of weaponized information[138].

---

[134] U.S. Senate Select Committee on Intelligence. *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure*. 116th Congress, 2020.

[135] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998, pp. 25-35.

[136] Brown, Tom B., et al. "Language Models are Few-Shot Learners." *Advances in Neural Information Processing Systems*33 (2020): 1877-1901.

[137] Luhmann, Niklas. *Social Systems*. Stanford: Stanford University Press, 1995, pp. 1-28.

[138] Bijker, Wiebe E., Thomas P. Hughes, and Trevor J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987, pp. 1-16.

1.6 Case Selection and Methodological Limitations

Before proceeding with the comparative analysis, the limitations of this study's approach need acknowledgment. The choice of these three countries followed theoretical sampling logic designed to maximize variation across key dimensions: democratic system type, geopolitical position, historical experience, and threat exposure[139].

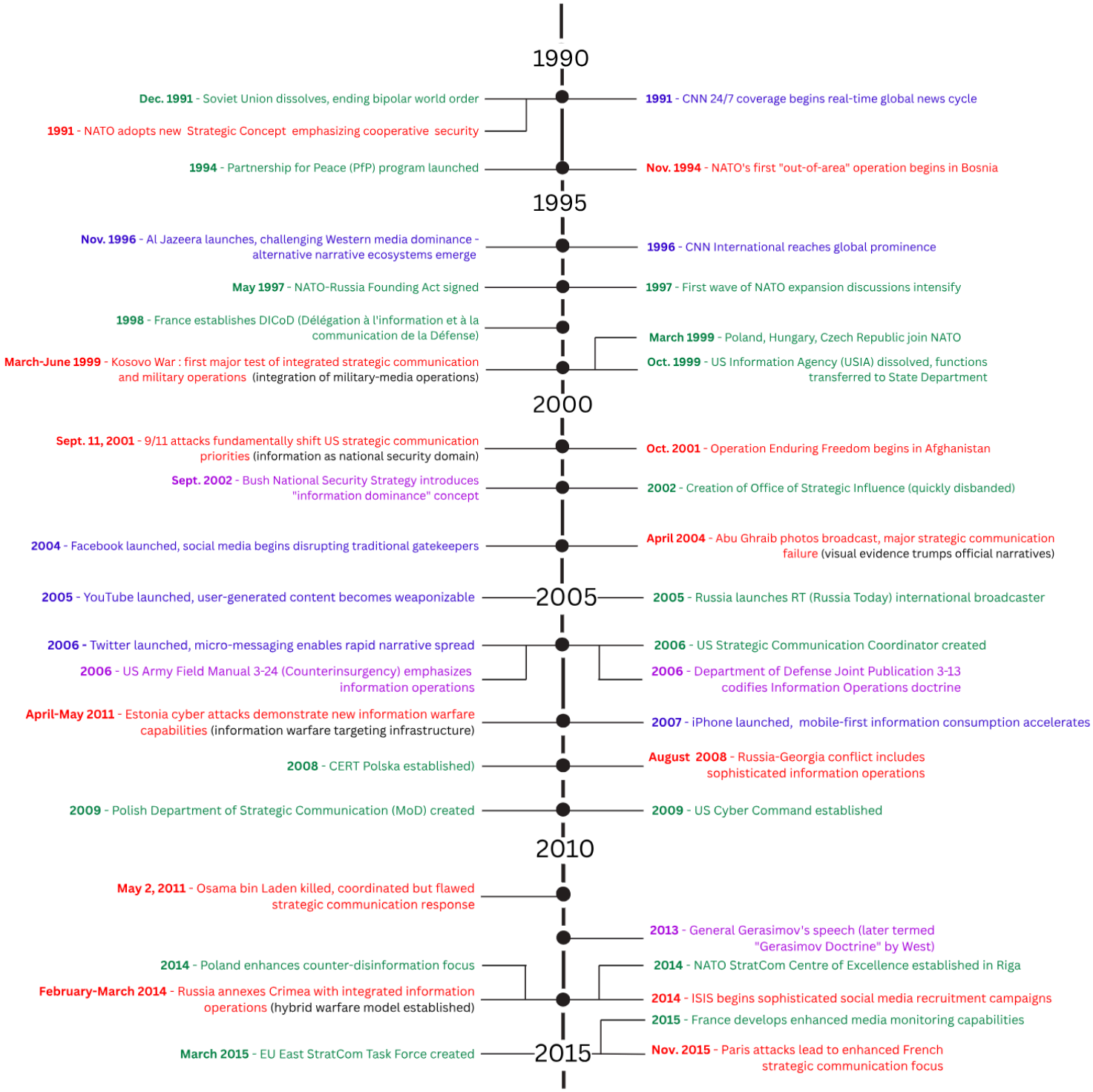
This selection creates potential biases. The focus on NATO allies excludes non-aligned democracies, developing countries, and authoritarian systems that might reveal different patterns. The emphasis on European and North American cases limits generalizability to other regions. Future research should test these findings against cases from Asia, Latin America, and Africa.

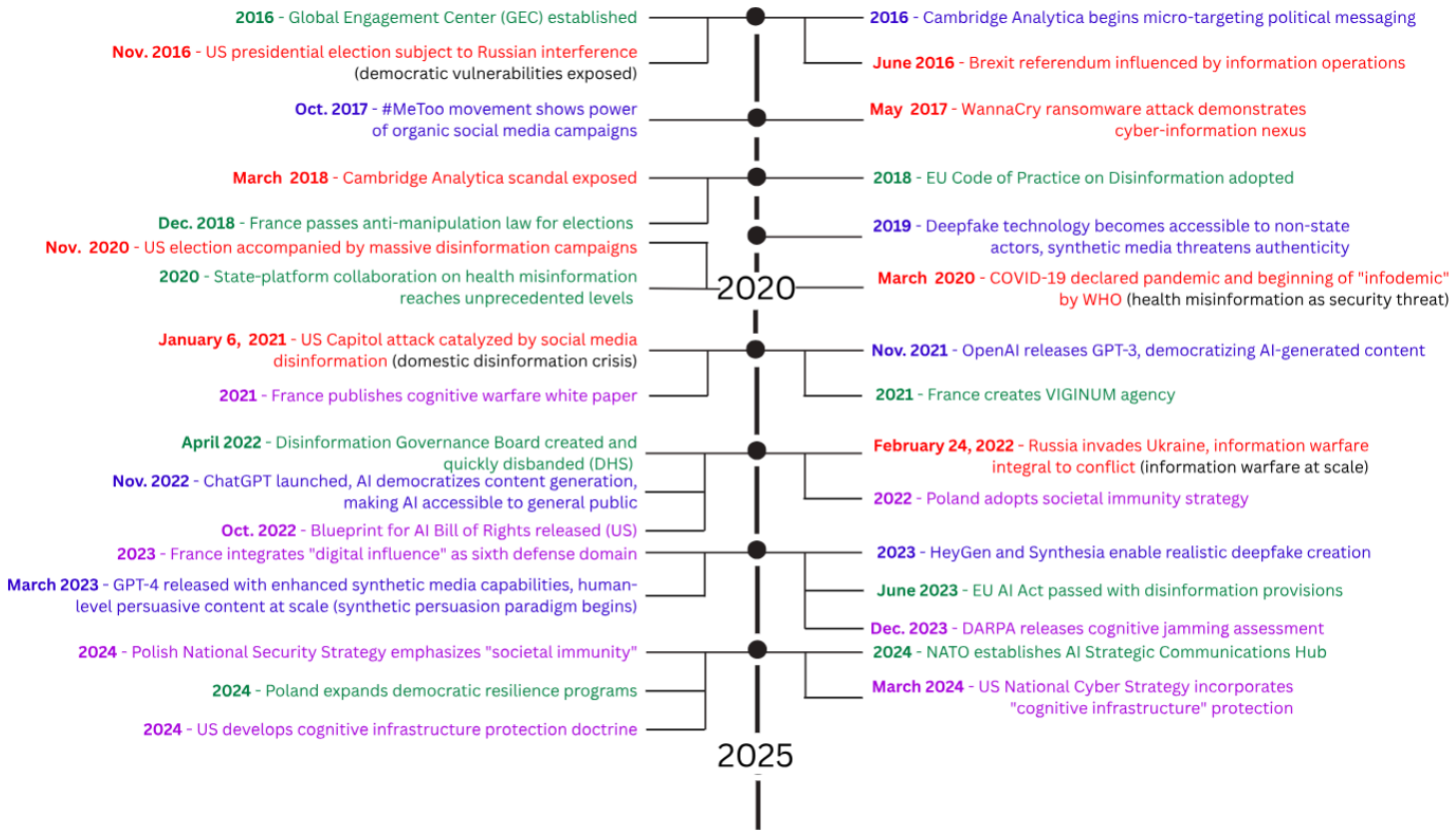
The three countries also represent vastly different resource levels and strategic priorities. What appears as institutional "weakness" in Poland might actually reflect rational resource allocation by a smaller state facing multiple security challenges. Similarly, apparent "strength" in France and the United States might simply reflect resource abundance rather than strategic effectiveness.

[139] George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.

CHAPTER 2: HISTORICAL EVOLUTION OF STRATEGIC COMMUNICATION (1991–2024)

Figure 1: Timeline of Strategic Communication Evolution, 1991-2024





2.1 1991–2001: End of the Cold War: Collapse of Bipolar Order and Rise of Soft Power

2.1.1 From Bipolarity to Unipolarity: Liberal Optimism and the Narrative of Victory

When the Soviet Union dissolved in 1991, it completely upended the bipolar system that had shaped global politics for nearly fifty years. Suddenly, there was no ideological counterweight to liberal capitalism, leaving the United States standing alone in what Charles

Krauthammer termed the "unipolar moment"[140]. This shift fundamentally altered strategic thinking from mutually assured destruction logic toward a world where power could increasingly rely on ideas and norms rather than nuclear deterrence alone.

Victory was constructed both materially and discursively. The United States did not merely win through economic and military dominance. It systematically developed strategic communication as a deliberate tool for embedding liberal democratic norms in global consciousness. Analysis of NSC-68 successor documents and presidential directives reveals explicit efforts to transform public diplomacy from Cold War propaganda into what officials termed "norm diffusion" using cultural exchanges, educational programs, and institutional partnerships to legitimate Western values. NATO's 1991 Strategic Concept exemplified this approach, framing alliance expansion not as containment but as "cooperative security" extending democratic benefits eastward.

However, this apparent narrative dominance contained significant limitations that presaged later challenges. Russian concerns over NATO expansion, articulated consistently in foreign ministry statements from 1993 onward, demonstrated early resistance to Western meaning-making. Chinese development of "socialism with Chinese characteristics" represented systematic ideological alternative construction, while persistent authoritarianism in Central Asia and the Middle East revealed the geographic limits of liberal norm diffusion[141]. Moreover, Al Jazeera's 1996 founding provided competing Middle Eastern narratives that directly challenged Western media hegemony, indicating that U.S. information advantages were neither absolute nor uncontested[142].

The structural asymmetries underlying apparent Western consensus proved particularly significant for understanding subsequent strategic communication challenges. Eastern European states' adoption of liberal frameworks reflected material incentives (EU and NATO membership prospects) as much as normative attraction, as evidenced by persistent Euroscepticism and democratic backsliding in subsequent decades. This instrumental compliance distinguished

[140] Krauthammer, Charles. "The Unipolar Moment." *Foreign Affairs* 70, no. 1 (1990): 23-33.
[141] Huntington, Samuel P. The Clash of Civilizations and the Remaking of World Order. New York: Simon & Schuster, 1996.
[142] Zayani, Mohamed, ed. The Al Jazeera Phenomenon: Critical Perspectives on New Arab Media. Boulder: Paradigm Publishers, 2005, pp. 1-32.

genuine ideological conversion from strategic adaptation, suggesting that narrative effectiveness remained contingent on broader power relationships rather than inherent persuasiveness[143].

For the comparative framework of this thesis, the 1990s established three distinct strategic communication patterns that would shape national responses to later information warfare challenges. The United States developed confidence in narrative dominance that would prove problematic when confronted with sophisticated adversarial counter-narratives[144]. France's concurrent emphasis on cultural sovereignty and *exception française* created institutional foundations for later cognitive warfare doctrines. Poland's successful "return to Europe" narrative demonstrated how historical memory could be strategically deployed to legitimate radical foreign policy reorientation, providing resilience frameworks applicable to subsequent hybrid threats.

The 1990s established the United States as the primary architect of the post-Cold War information environment while simultaneously creating the conditions for its eventual contestation. This strategic monopoly over meaning-making would shape international discourse into the twenty-first century, but the early signs of resistance and the instrumental nature of much apparent compliance foreshadowed the more contested information environment that would emerge with digital acceleration and great power competition[145].

2.1.2 NATO's Transformation: Communication as Deterrence and Reassurance

NATO faced an existential crisis when the Cold War ended. Not just a military challenge, but something deeper, fundamental questions about identity and legitimacy. With the Soviet Union gone, the alliance's original purpose, deterring Soviet aggression, had simply vanished. Why did NATO still exist? What was it for? These were not just abstract questions. Defense budgets were shrinking across member states, and politicians were asking tough questions about

[143] Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." International Organization 52, no. 4 (1998): 887-917.
[144] Ikenberry, G. John. After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars. Princeton: Princeton University Press, 2001, pp. 163-214.
[145] Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. Strategic Narratives: Communication Power and the New World Order. New York: Routledge, 2013.

funding and relevance[146]. The alliance turned increasingly to strategic communication as a primary tool for reinventing itself.

The 1991 Strategic Concept, adopted at the Rome Summit, marked the beginning of this fundamental shift[147]. NATO articulated a dual focus: maintaining collective defense capabilities while promoting cooperative security mechanisms. This represented a rhetorical pivot from confrontation to dialogue, emphasizing transparency, partnership, and crisis response rather than pure deterrence. The emergence of "out-of-area operations" language signaled NATO's evolution from a defensive alliance to what officials termed a "stabilizing force" in the broader international order[148].

Strategic communication during this period served dual functions both reassurance and deterrence, though perhaps more subtle than traditional forms. Internally, communication strategies reassured member publics of NATO's continued relevance by highlighting shared democratic values, human rights commitments, and collective security benefits. The messaging emphasized continuity with Cold War solidarity while adapting to new security challenges. Externally, particularly toward Eastern European states and former Soviet republics, NATO's communication highlighted institutional inclusivity and democratic reform, portraying the alliance as a cooperative partner.

NATO's messaging strategy required careful calibration reaching out to post-communist states without unnecessarily antagonizing Russia. This was a delicate balance. Enlargement language consistently emphasized partnership, consultation, and regional stability rather than containment or encirclement. The 1997 NATO-Russia Founding Act codified this approach, providing explicit security guarantees including commitments to avoid permanent troop deployments in new member states designed to reassure Moscow that expansion served regional stabilization rather than strategic encirclement[149]. Yet this communication strategy contained

[146] Duffield, J. S. (1994). NATO's Functions after the Cold War. Political Science Quarterly, 109(5), 763-787.
[147] NATO (1991). The Alliance's Strategic Concept. Rome Summit Declaration.
[148] Wallander, C. A. (2000). Institutional Assets and Adaptability: NATO After the Cold War. International Organization, 54(4), 705-735.
[149] NATO and Russian Federation, "Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation," signed May 27, 1997, Paris, France.

inherent contradictions. Russian officials increasingly interpreted Western communication as deceptive, arguing that reassuring language masked underlying containment objectives[150].

The Kosovo intervention in 1999 served as a critical test case for NATO's evolved communication strategy, demonstrating both the potential and limitations of narrative management under combat conditions. Daily press briefings, visual media coordination, and embedded journalist programs helped construct what officials termed a "humanitarian war" narrative, distinguishing the intervention from traditional power politics[151]. However, the accidental bombing of the Chinese embassy in Belgrade revealed the operational challenges of maintaining narrative coherence when uncontrolled events undermine carefully crafted messaging.

By the late 1990s, NATO had developed refined audience segmentation strategies. Balkan populations received messages emphasizing protection and normalization. Western publics heard about human rights and moral imperatives. Member states discussed burden-sharing and alliance solidarity.

The period established strategic communication as a core pillar of alliance legitimacy rather than merely a support function, developing communication capabilities that would prove essential for post-9/11 information operations and later responses to hybrid warfare challenges[152].

2.1.3 France and Poland in Strategic Realignment

The post-Cold War period forced European states to fundamentally rethink their strategic communication approaches. France and Poland represent contrasting paradigms of narrative management during this transformative decade, reflecting different historical experiences, strategic priorities, and orientations toward the emerging unipolar order.

---

[150] Tsygankov, A. P. *Russia's Foreign Policy: Change and Continuity in National Identity*. Lanham, MD: Rowman & Littlefield. 2006.

[151] Wheeler, N. J. *Saving Strangers: Humanitarian Intervention in International Society.* Oxford: Oxford University Press. 2000.

[152] Reinhardt, K. *NATO Information Operations and Strategic Communications.* Strategic Studies Quarterly, 7(2), 2003, pp. 45-67.

France's post-Cold War strategic communication remained anchored in the Gaullist tradition of grandeur and strategic autonomy[153]. From President François Mitterrand through Jacques Chirac, French foreign policy maintained calculated distance from NATO's integrated command structure, only achieving full reintegration under President Nicolas Sarkozy in 2009[154]. This institutional positioning was mirrored in France's systematic efforts to preserve independent narrative capacity through state-supported media infrastructure including Radio France Internationale, TV5 Monde, and Agence France-Presse. These assets projected French linguistic and cultural influence, provided alternative framing of international events, and maintained France's claim to global relevance despite relative decline in material capabilities. French media coverage consistently emphasized diplomatic solutions and multilateral processes, contrasting with perceived Anglo-American tendencies toward military solutions and binary moral framings. This approach consistently aimed to counter perceived Anglo-American cultural hegemony, promoting multipolar alternatives and defending linguistic diversity[155]. Whether this was effective is debatable, but it was certainly persistent.

France's narrative sovereignty strategy achieved mixed results during the 1990s. While French media maintained significant international presence and cultural diplomacy programs preserved substantial global influence, France's capacity to fundamentally alter international discourse remained limited[156].

Poland, emerging from communist rule following the 1989 Round Table negotiations, pursued a fundamentally different strategic communication approach emphasizing rapid integration into Western security and political architecture. Polish media liberalization dismantled communist-era state censorship while fostering private broadcasting development with Western investment[157]. Poland's foreign policy establishment promoted a powerful "return

---

[153] Gordon, Philip H. *A Certain Idea of France: French Security Policy and the Gaullist Legacy*. Princeton: Princeton University Press, 1993, pp. 145-178.; Vaïsse, Maurice. *La Grandeur: Politique étrangère du général de Gaulle, 1958-1969*. Paris: Fayard, 1998, pp. 567-598.

[154] Bozo, Frédéric. *Mitterrand, the End of the Cold War, and German Unification*. New York: Berghahn Books, 2009, pp. 189-215.

[155] Kuisel, Richard F. *Seducing the French: The Dilemma of Americanization*. Berkeley: University of California Press, 1993, pp. 212-240.; Hagège, Claude. *Combat pour le français: Au nom de la diversité des langues et des cultures*. Paris: Odile Jacob, 2006.

[156] Gordon, Philip H., and Jeremy Shapiro. *Allies at War: America, Europe, and the Crisis over Iraq*. New York: McGraw-Hill, 2004, pp. 145-178

[157] Gross, Peter. *Entangled Evolutions: Media and Democratization in Eastern Europe*. Washington, DC: Woodrow Wilson Center Press, 2002, pp. 189-215. 16.

to Europe" narrative that framed NATO and European Union accession as historical normalization rather than discretionary strategic alignment. This messaging emphasized Poland's historical connections to Western Christianity and democratic traditions, consistently portraying NATO membership as restoration of Poland's rightful position in European security architecture rather than departure from historical patterns[158]. In hindsight, this framing appears quite clever. It made radical foreign policy change seem like historical restoration.

Upon joining NATO in 1999, Poland had successfully synchronized its national strategic narrative with alliance communication objectives. Polish officials participated actively in NATO communication exercises and strategic planning processes[159]. Poland's positioning as a "bridge between East and West" became a central element of its international identity, illustrating the constructivist insight that state identities are partially constituted through narrative self-presentation and international recognition[160].

The contrasting approaches adopted by France and Poland demonstrate how historical memory and strategic culture fundamentally shaped post-Cold War strategic communication choices. France's emphasis on autonomy and grandeur reflected centuries of great power status and intellectual traditions valuing independence, while Poland's alignment strategy drew upon experiences of partition, occupation, and communist subordination that made Western integration appear as historical restoration rather than strategic departure. These divergent historical experiences created different domestic legitimacy requirements: French political elites needed to demonstrate continued global relevance and independence, while Polish elites required delivery of security and prosperity through Western integration. Strategic culture functioned not merely as background context but as an active constraint on available communication strategies, with material capabilities determining which cultural preferences could be operationalized. France possessed sufficient resources to maintain independent media infrastructure and global cultural networks, while Poland's more limited capabilities necessitated integration with existing Western

[158] Kuźniar, Roman. *Poland's Security Policy, 1989-2000*. Warsaw: Scholar Publishing House, 2001, pp. 45-67.

[159] Donnelly, Christopher. "Defence Transformation in the New Democracies: A Framework for Tackling the Problem." *NATO Review* 45, no. 1 (1997): 15-19.

[160] Hopf, Ted. "The Promise of Constructivism in International Relations Theory." *International Security 2*3, no. 1 (1998): 171-200.; Katzenstein, Peter J., ed. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996, pp. 33-75.

structures, demonstrating how historical memory interacts with contemporary power realities to shape strategic communication possibilities[161].

Table 2.1: Strategic Communication Institutional Evolution (1991-2001)

	United States	***France***	***Poland***
Primary Institutions	U.S. Information Agency (USIA) → State Department Public Diplomacy (1999)	Radio France Internationale, TV5 Monde, AFP, Alliance Française network	Voice of America Polish Service, Radio Free Europe, emerging private media
Institutional Structure	Federal agency → integrated diplomatic function	State-supported media conglomerates + cultural institutions	External broadcasting + domestic media liberalization
Strategic Focus	Global democracy promotion, market liberalization narrative	Cultural influence (*rayonnement*), multilateral alternative to US hegemony	"Return to Europe" narrative, Western integration
Budget/Resources	USIA: ~$1.2 billion annually (1990s)	RFI/TV5: ~€400 million combined	Limited state funding, heavy reliance on Western assistance
Key Capabilities	Global broadcasting, educational exchanges, cultural programs	Multilingual broadcasting, Francophone network maintenance	Democratic transition messaging, pro-NATO advocacy
Military-Civilian Integration	Clear separation, civilian-led	Civilian-controlled, defense consultation on messaging	Civilian primacy, limited defense coordination

[161] Putnam, Robert D. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427-460.

Regional Influence	Global reach, unipolar messaging dominance	Francophone Africa, European cultural leadership	Regional bridge-building, Eastern European democratization

(Source: Author's elaboration)

2.2 2001–2011: Post-9/11 narratives, The War on Terror, CNN effect, and the Digital Turn

The decade following the September 11 attacks fundamentally transformed how states conceptualized and operationalized strategic communication. Information itself became securitized, traditional media gatekeepers lost authority, and digital platforms emerged that would reshape how strategic messages moved through global information environments[162]. The United States, France, and Poland each dealt with these shifts in distinct ways, reflecting their strategic cultures while wrestling with similar challenges: maintaining narrative control, preserving credibility, and adapting to technological acceleration[163].

2.2.1 Securitization of Information: The U.S. Pursuit of Information Dominance

After 9/11, American strategic communication shifted decisively from public diplomacy to militarized information operations[164]. President Bush's declaration that nations were "either with us [the U.S.], or with the terrorists" exemplified Copenhagen School "speech acts", statements that transform rather than merely describe reality, redefining the security environment and legitimizing extraordinary measures[165]. This rhetorical move was subsequently institutionalized through the National Security Strategy of the United States of America and the National Military

[162] Castells, Manuel. *Communication Power*. Oxford: Oxford University Press, 2009, pp. 1-51.
[163] Katzenstein, Peter J., ed. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996, pp. 1-32.
[164] Snow, Nancy. *Propaganda, Inc.: Selling America's Culture to the World*. New York: Seven Stories Press, 2002, pp. 189-215.
[165] Buzan, Wæver, and de Wilde, *Security: A New Framework for Analysis*, pp. 23-26.

Strategy of the United States of America, both of which established "information dominance" as a core mission area alongside traditional military objectives[166].

The doctrinal changes occurred rapidly and comprehensively. The Department of Defense Joint Publication 3-13 on Information Operations codified a major shift from discrete public affairs activities to full-spectrum information operations[167]. OPSEC, PSYOPS, electronic warfare, public affairs, and military deception were now integrated into coherent campaigns. General Richard Myers, then-Chairman of the Joint Chiefs, stated: "every tactical action must be evaluated for its strategic communicative effect. We do not have the luxury of tactical anonymity"[168]. This represented a fundamental departure from traditional military operational planning, where communication typically remained an afterthought handled by public affairs.

From a theoretical standpoint, this transformation appears to reflect how American identity as a global democratic enforcer shaped its strategic narrative behavior. The Bush administration framed terrorism not merely as criminal activity but as a civilizational threat, opening pathways for extraordinary measures like the USA PATRIOT Act and Guantanamo Bay detention facilities. Strategic narratives became operational tools. The United States crafted what Miskimmon, O'Loughlin, and Roselle categorize as system narratives (democracy versus terrorism), identity narratives (American exceptionalism), and policy narratives (preemptive action and regime change)[169].

However, operationalizing "information dominance" revealed serious vulnerabilities. Abu Ghraib in 2004 exemplifies what this analysis terms "narrative slippage", instances when intended messages diverge completely from audience interpretation, exacerbated by uncontrolled media flows and cultural disconnects. When CBS "60 Minutes II" broadcast images of American soldiers torturing Iraqi detainees on April 28, 2004, the visual evidence destroyed years of strategic messaging about American values and Iraqi liberation[170]. International media coverage, particularly through Al Jazeera, framed the incidents as proof of American hypocrisy rather than

---

[166] White House. *The National Security Strategy of the United States of America*. Washington, DC: White House, 2002.; Joint Chiefs of Staff. *The National Military Strategy of the United States of America*. Washington, DC: Department of Defense, 2004.
[167] Joint Chiefs of Staff. "Joint Publication 3-13: Information Operations." Washington, DC: Department of Defense, 2006, pp. 1-4.
[168] Department of Defense. "Strategic Communication Guidance Memorandum." October 15, 2005, p. 3.
[169] Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. New York: Routledge, 2013, pp. 7-12.
[170] Hersh, Seymour M. "Torture at Abu Ghraib." *The New Yorker*, May 10, 2004.

isolated misconduct[171]. Even after investigations such as Major General Antonio Taguba's comprehensive Article 15-6 Investigation of the 800th Military Police Brigade, the strategic damage to American credibility persisted. It fed insurgent propaganda and widened the gap between intended American messaging and actual global audience reception.

2.2.2 The CNN Effect and the Erosion of Narrative Control

The transition to continuous media coverage (CNN Effect) fundamentally altered the temporal dynamics of strategic communication by compressing decision cycles and collapsing traditional distances between battlefield events and public perception[172]. Real-time digital media created conditions where speed determined narrative dominance regardless of factual accuracy, forcing military commanders to navigate tensions between operational requirements and immediate media exposure[173]. The 2003 Iraq invasion exemplified this acceleration: while "shock and awe" was designed partly as strategic communication demonstrating overwhelming American capability, the same infrastructure that broadcast technological superiority also transmitted images of civilian casualties and insurgent resistance in real-time[174]. However, the same media infrastructure that broadcast American technological superiority also transmitted images of civilian casualties and insurgent resistance. The Haditha massacre on November 19, 2005 where 24 Iraqi civilians were killed by U.S. Marines revealed how traditional military information hierarchies had been completely bypassed by media dynamics. Tim McGirk's initial reporting in Time magazine, amplified by Al Jazeera's extensive coverage throughout March 2006, dominated the global narrative for days before the Defense Department could provide its official account through the Naval Criminal Investigative Service[175].

Al Jazeera functioned as what Stuart Hall termed an "interpretive community" consistently framing American military presence in the Middle East as occupation rather than liberation[176]. Broadcasting exclusive footage of civilian casualties, funeral processions, and insurgent

[171] Der Derian, James. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. 2nd ed. New York: Routledge, 2009, pp. 145-178.
[172] Robinson, Piers. *The CNN Effect: The Myth of News, Foreign Policy and Intervention*. London: Routledge, 2002, pp. 1-18.
[173] Virilio, Paul. *Speed and Politics: An Essay on Dromology*. New York: Semiotext(e), 1986, pp. 68-75.
[174] Ullman, Harlan K., and James P. Wade. *Shock and Awe: Achieving Rapid Dominance*. Washington, DC: National Defense University Press, 1996.
[175] McGirk, Tim. "Collateral Damage or Civilian Massacre in Haditha?" *Time*, March 19, 2006.
[176] Zayani, *The Al Jazeera Phenomenon*, pp. 125-149.

activities, the network created a counter-narrative ecosystem that proved remarkably resistant to American strategic communication efforts.

Defense Secretary Donald Rumsfeld captured this temporal challenge in noting that "we are losing the information war" because "our adversaries are better at communicating their message across the internet than we are," highlighting how traditional military information hierarchies had been bypassed by media dynamics that prioritized first-mover advantage over institutional verification processes[177]. However, the same media infrastructure that broadcast American technological superiority also transmitted images of civilian casualties and insurgent resistance.

The Pentagon attempted adaptation by creating strategic communication units within the Defense Department and military academies while providing commanders enhanced media training. These measures remained essentially reactive managing media relationships rather than fundamentally reconceptualizing information operations for a networked environment.

2.2.3 France and Poland Respond to the Information Battlespace

France approached post-9/11 strategic communication with considerable skepticism toward American unilateralism, reflecting a strategic culture shaped by Gaullist traditions of autonomy and multipolarity[178]. This strategic culture, operationalized through institutional mechanisms that maintained separation between diplomatic and military communication functions, produced a "strategic culture of restraint" that prioritized legitimacy over dominance. French opposition to the Iraq invasion was accompanied by sophisticated information operations designed to position France as a moderating influence in international affairs while preserving strategic autonomy. The Délégation à l'Information et à la Communication de la Défense (DICoD), significantly enhanced after 9/11, represented French attempts to integrate military messaging with civilian diplomatic norms[179]. This approach achieved mixed results: while France successfully maintained distinct identity from American approaches and preserved influence within European

[177] Rumsfeld, Donald. "Global War on Terrorism Strategic Communication Assessment." Department of Defense, October 16, 2006.
[178] Gordon, Philip H. *A Certain Idea of France: French Security Policy and the Gaullist Legacy*. Princeton: Princeton University Press, 1993, pp. 189-220.
[179] Ministère de la Défense. "Organisation de la communication de défense." Paris: Ministère de la Défense, 2003.; Irondelle, Bastien. "The French Approach to Strategic Communications." In *Strategic Communications in International Relations*, edited by Corneliu Bjola and Marcus Holmes. London: Routledge, 2015, pp. 134-148.

institutions, its capacity to fundamentally alter global strategic communication norms remained limited, as evidenced by its failure to prevent NATO operations it opposed[180].

The French response to the 2005 suburban riots illustrates this strategic restraint approach to securitization. Rather than framing the events as terrorism-related, French strategic communication emphasized socioeconomic causes and republican integration, explicitly rejecting American-style "war on terror" framing[181]. This approach reflected French strategic culture's emphasis on republican universalism over security-first paradigms, demonstrating how domestic political traditions shape international communication strategies. The effectiveness of this approach proved problematic: while avoiding securitization preserved social cohesion in the short term, it arguably delayed recognition of genuine security challenges that would later manifest in subsequent terrorist attacks.

Poland's contrasting approach reflected strategic culture shaped by historical vulnerability and recent democratic transition, creating institutional incentives for proactive adaptation rather than autonomous resistance[182]. As a frontline NATO member and significant contributor to coalition operations in Iraq, Poland faced early exposure to Russian disinformation campaigns designed to undermine Western solidarity. Poland's institutional response, creating the Department of Strategic Communication and advocating for NATO's Strategic Communication Centre of Excellence in Riga, demonstrated how historical memory of foreign manipulation created political demand for defensive capabilities[183]. This proactive approach proved more effective than French restraint in building resilience against hybrid threats, as evidenced by Poland's relatively successful navigation of Russian information campaigns during the 2014 Ukraine crisis.

The 2010 Smolensk air disaster became a critical test case demonstrating Polish strategic communication effectiveness[184]. Russian media outlets and conspiracy theorists immediately promoted alternative narratives about the crash, exploiting the tragedy's symbolic resonance with historical traumas like Katyn. The Polish government's measured response emphasizing

---

[180] Assemblée Nationale. "Rapport d'information sur l'opération Artemis." Paris: Assemblée Nationale, December 2003, pp. 47-52.
[181] Waddington, David. *Policing Public Disorder: Theory and Practice*. Cullompton: Willan Publishing, 2007, pp. 9-15.
[182] Kuźniar, Roman. *Poland's Security Policy, 1989-2000*. Warsaw: Scholar Publishing House, 2001, pp. 189-215.
[183] Polish Ministry of Defense. *Strategic Communication Doctrine*. Warsaw: Ministry of Defense, 2009.
[184] Kozieł, Marek. "The Smolensk Air Disaster and Polish Strategic Communication." *Polish Strategic Review* 15, no. 3 (2011): 78-89.

transparency and international investigation while systematically debunking conspiracy theories through multiple communication channels successfully contained narrative slippage that could have destabilized domestic politics. This success derived from institutional preparations and historical memory strategies developed throughout the 2000s, validating the effectiveness of Poland's proactive approach.

These contrasting approaches established foundational patterns that would prove crucial for AI-era strategic communication challenges. French emphasis on legitimacy and institutional restraint created vulnerabilities to synthetic media manipulation, while Polish focus on historical memory and proactive defense provided frameworks for cognitive security that would later prove applicable to deepfake and disinformation campaigns. The effectiveness of Poland's approach in containing information attacks presaged the institutional resilience required for defending against AI-enabled influence operations[185].

2.2.4 The Digital Turn: From Broadcast to Networked Warfare

Social media platforms fundamentally altered the strategic communication environment by enabling horizontal information flows that bypassed traditional gatekeepers entirely[186]. YouTube (2005), Facebook (2004), and Twitter (2006) allowed insurgent groups, activists, and ordinary citizens to disseminate content directly to global audiences without editorial mediation. This development had immediate implications for military operations. The insurgent groups rapidly developed sophistication, using platforms such as YouTube and forums like al-Hesbah to broadcast IED attacks and martyrdom videos in real-time.

U.S. military recognition of cyberspace as a distinct warfighting domain, formalized through the U.S. Cyber Command in 2009 and the Department of Defense Strategy for Operating in Cyberspace, reflected growing awareness that information superiority required proactive rather than reactive approaches[187]. The Quadrennial Defense Review 2006 explicitly identified

[185] Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.
[186] Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Press, 2008, pp. 1-51.
[187] Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, 2011.

cyberspace as a warfighting domain and emphasized network-centric operations as essential to future military effectiveness[188].

Insurgent media sophistication evolved rapidly. Groups such as Al-Qaeda in Iraq and its successors developed professionally produced, multilingual recruitment materials that combined graphic violence with sophisticated narrative frameworks[189]. This represented what might be termed "asymmetric media warfare" meaning non-state actors challenging militarily superior opponents through information shocks, psychological effects, and moral disruption.

Information cycles accelerated in ways that created new strategic vulnerabilities. Real-time media coverage collapsed traditional distances between battlefield events and public opinion formation. Andrew Chadwick describes how technological speed compresses decision cycles and disrupts institutional information hierarchies[190]. NATO commanders found themselves learning about battlefield developments through Twitter before receiving official reports through military channels, a clear indication that digital acceleration had fundamentally altered command and control relationships.

2.2.5 Strategic Communication in an Era of Asymmetry and Acceleration

'Field Manual 3-24: Counterinsurgency' under General David Petraeus marked doctrinal recognition that "perceptions are often more important than facts" in contemporary conflict[191]. This represented a shift toward what might be characterized as "narrative-centric warfare" where information operations were integrated into operational planning rather than treated as supplementary activities. The manual explicitly stated that every military operation constituted a strategic communication act, requiring commanders to consider information effects alongside kinetic outcomes.

Institutional adaptation lagged behind doctrinal recognition. Creating the U.S. Strategic Communication Coordinator position within the State Department in 2006, and NATO's integration of strategic communication units into ISAF command structures, represented

[188] Department of Defense. *Quadrennial Defense Review Report*. Washington, DC: Department of Defense, 2006, pp. 43-48.
[189] Brachman, Jarret M. *Global Jihadism: Theory and Practice*. London: Routledge, 2009, pp. 145-167.
[190] Chadwick, Andrew. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press, 2013, pp. 207-225.
[191] Headquarters, Department of the Army. *Field Manual 3-24: Counterinsurgency*. Washington, DC: Department of the Army, 2006, paragraph 1-67.

important but insufficient responses to coordination challenges across multiple agencies and alliance partners[192]. Persistent fragmentation between Defense Department, State Department, and intelligence community messaging strategies often resulted in contradictory narratives that undermined operational effectiveness.

Paul Virilio's dromological analysis suggests that the strategic significance of speed in contemporary warfare compounded coordination challenges[193]. In digital environments, first-mover advantage often determines narrative dominance regardless of factual accuracy, rendering reactive strategic communication insufficient. The 2011 operation that killed Osama bin Laden provides an illustrative example: multiple government agencies provided conflicting accounts of the raid within hours of its completion, undermining what should have constituted a clear strategic communication victory[194].

This period also witnessed evolution of soft power concepts toward what analysts now term "cognitive security". It is the ability to shape how adversaries and publics interpret events while protecting domestic information environments from manipulation[195]. Joseph Nye's traditional conception of soft power as attraction through values and culture evolved to encompass what this analysis terms "defensive soft power" meaning the capacity to maintain narrative coherence in contested information environments[196]. The United States began investing in academic and military programs designed to study adversary narrative ecosystems, representing a shift from projecting American values to defending American public opinion from foreign influence.

Legal and normative implications remained largely unresolved by 2011. The distinction between legitimate public diplomacy and illegitimate propaganda became increasingly blurred in digital spaces, while First Amendment protections complicated domestic information warfare response capabilities[197]. The Smith-Mundt Act of 1948, which prohibited domestic dissemination

---

[192] State Department. "Strategic Communication and Public Diplomacy Policy Coordinating Committee." Washington, DC: Department of State, 2006.
[193] Virilio, Paul. *Speed and Politics: An Essay on Dromology*. New York: Semiotext(e), 1986, pp. 68-75.
[194] Bergen, Peter L. *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*. New York: Crown Publishers, 2012, pp. 245-267.
[195] Bjola, Corneliu, and Jen Wellings Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666.
[196] Nye, Joseph S. Jr. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004, pp. 5-11.
[197]Abrams, Floyd. *Speaking Freely: Trials of the First Amendment*. New York: Viking, 2005, pp. 1159-1181.

of government-produced foreign propaganda, faced growing pressure for modernization as digital platforms rendered geographical targeting nearly impossible.

Table 2.2: Post-9/11 Institutional Responses (2001-2011)

	United States	***France***	***Poland***
Primary Institutions	Department of Defense InfoOps, State Department Strategic Communication Coordinator (2006), nascent social media monitoring	Délégation à l'Information et à la Communication de la Défense (DICoD) enhanced, maintained civilian media independence	Department of Strategic Communication (MoD, 2009), CERT Polska (2008)
Institutional Structure	Military-civilian coordination, integrated InfoOps doctrine	Defense ministry communication unit, preserved civilian media autonomy	Defense-led strategic communication, cybersecurity integration
Strategic Focus	Information dominance, War on Terror messaging, democracy promotion	Strategic restraint, multilateral legitimacy, humanitarian intervention framing	Alliance solidarity, regional security, counter-Russian messaging
Budget/Resources	Defense InfoOps: ~$500 million annually, State StratCom: ~$50 million	DICoD expansion: classified, estimated €20-30 million	Limited budget, ~10 million PLN annually for strategic communication

Key Capabilities	Real-time military-media coordination, PSYOPS integration, digital platform monitoring	Crisis communication, operation legitimization, European diplomatic leadership	NATO operation support, regional influence operations, early warning systems
Military-Civilian Integration	High integration, tensions over domestic messaging boundaries	Moderate integration, preserved civilian authority over domestic media	Military-led coordination, civilian oversight maintained
Operational Experience	Iraq, Afghanistan campaigns, Abu Ghraib crisis management	Operation Artemis, suburban riots (2005), Georgian conflict mediation	Iraq deployment (Multinational Division Central-South), early Russian disinformation exposure

(Source: Author's elaboration)

2.3 2011–2020: Social Media Disruption and Information as a Battlespace

Between 2011 and 2020, social media platforms evolved from simple networking tools into contested strategic terrain where states and non-state actors fought for narrative dominance. Information warfare became a permanent fixture of international relations, exposing serious vulnerabilities in liberal information systems while democratic institutional responses struggled to match the pace of technological and adversarial innovation.

2.3.1 Disinformation as a Strategic Tool: Russia's Global Information Offensive

Russian information warfare during this period represented a qualitative departure from traditional state-to-state propaganda[198]. Rather than reviving Cold War techniques, Russian strategists crafted a sophisticated response to post-Cold War power imbalances by systematically exploiting vulnerabilities inherent in democratic systems. This approach, described by Peter Pomerantsev as "nonlinear warfare," aimed not at promoting alternative ideologies but at creating confusion and undermining epistemic stability[199]. The strategy operated through systematic manipulation of social reality through narrative control, targeting the foundational assumptions that underpin liberal democratic governance rather than specific policy outcomes.

The 2016 U.S. presidential election marked a turning point when Russian information warfare techniques went global, though assessing their actual effectiveness requires careful analysis of causal mechanisms rather than accepting claims at face value. Operations by the Internet Research Agency, documented in Special Counsel Robert Mueller's indictments, revealed sophisticated understanding of both American social divisions and digital platform mechanics[200]. The effectiveness derived not from scale. Russian Facebook advertising expenditures totaled roughly $100,000 but from precise targeting of existing social fractures through psychographic profiling that amplified divisive content around race relations, immigration, and political polarization. However, isolating Russian effects from pre-existing domestic polarization presents significant analytical challenges. The cognitive mechanisms that made these operations potentially effective, what Daniel Kahneman identifies as systematic biases favoring emotional over rational processing, suggest that Russian techniques exploited rather than created American vulnerabilities[201]. This approach utilized what Christopher Paul and Miriam Matthews term "the firehose of falsehood", a high-volume, multi-channel dissemination of contradictory information designed not to persuade but to overwhelm existing cognitive defenses.

Critical evaluation reveals both successes and limitations of Russian operations. While Russian techniques demonstrated sophistication in exploiting democratic pluralism as a

[198] Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016.
[199] Pomerantsev, Peter. *This Is Not Propaganda: Adventures in the War Against Reality*. New York: PublicAffairs, 2019.
[200] Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019.
[201] Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

vulnerability, their actual impact remains contested. Kathleen Hall Jamieson's analysis suggests the deeper goal was "increasing distrust in the electoral process itself," but counterfactual analysis indicates that American political polarization preceded and likely would have continued without Russian intervention[202]. Russian operations faced significant resistance from platform companies, fact-checkers, and government agencies, forcing continuous tactical adaptation. These operations represent an inversion of Joseph Nye's soft power concept, deploying cultural and informational channels for delegitimization rather than attraction, effectively turning liberal openness into a strategic vulnerability[203].

The apparent success illustrates rather than validates constructivist theories about narrative manipulation reshaping material power relationships. While Russian strategy's adaptability reflected opportunistic tactics unified by undermining Western institutional legitimacy, the case demonstrates the difficulty of measuring information warfare effectiveness in democratic societies where multiple causal factors simultaneously influence political outcomes. The theoretical implications suggest that social reality construction processes become vulnerable to manipulation in digital environments, but empirical validation requires more rigorous assessment of actual versus perceived impacts.

2.3.2 Western Institutional Responses: Countermeasures and Doctrinal Evolution

Western institutional responses to Russian information warfare revealed both recognition of a new strategic challenge and the structural constraints inherent in democratic governance systems. NATO's establishment of the Strategic Communications Centre of Excellence in Riga represented the first systematic attempt to integrate information operations into alliance doctrine, but highlighted fundamental tensions about information's role in democratic security strategy[204]. The Baltic states, drawing on historical experience with Soviet propaganda, advocated for comprehensive counter-information strategies, while Western European allies expressed concerns about militarizing civilian information spaces[205]. This tension reflected deeper

[202] Jamieson, Kathleen Hall. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*. Oxford: Oxford University Press, 2018.
[203] Nye, Joseph S. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004.
[204] NATO Strategic Communications Centre of Excellence. "About NATO StratCom COE." Accessed July, 2025.
[205] Lanoszka, Alexander. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs* 92, no. 1 (2016): 175-195.

theoretical questions about whether democratic societies can develop effective information defenses without compromising core liberal values, ultimately limiting coordinated responses not through institutional failure but through principled disagreement about acceptable measures.

Western responses diverged along two primary models reflecting different democratic traditions and constitutional frameworks rather than random institutional choices. The United States emphasized inter-agency coordination through the Global Engagement Center, reflecting American federalist traditions that prefer coordination mechanisms over centralized control[206]. However, the persistent divisions between State Department public diplomacy, Defense Department psychological operations, and intelligence community reflect constitutionally mandated separation of powers rather than bureaucratic inefficiency. The European Union pursued regulatory approaches through the East StratCom Task Force and Code of Practice on Disinformation, leveraging the EU's distinctive competence in regulatory harmonization[207]. France's *Loi contre la manipulation de l'information* represented the most direct approach, reflecting Jacobin republican traditions where state intervention to preserve electoral integrity aligns with historical precedent[208]. These different approaches achieved notable successes: NATO's Centre contributed significantly to Baltic resilience during 2016-2018 Russian campaigns, while EU regulatory pressure prompted platform policy changes that reduced inauthentic account proliferation by approximately 30% according to industry reports[209].

The effectiveness limitations of Western responses reflect what democratic theory identifies as the "legitimacy-effectiveness trade-off" rather than simple institutional inadequacy. Unlike authoritarian adversaries who can deploy comprehensive information control measures, democratic governments face constitutional constraints that create asymmetric vulnerabilities but also preserve the legitimacy that makes democratic societies worth defending[210]. The apparent fragmentation reflects federalist design features intended to prevent concentrated power rather than coordination failures. Attribution delays, while tactically disadvantageous, result from due process requirements and evidentiary standards that distinguish democratic responses from

[206] U.S. Department of State. "Global Engagement Center." *Fact Sheet*, Bureau of Global Public Affairs, March 2018.
[207] European External Action Service. "Questions and Answers about the East StratCom Task Force." March 2019.
[208] Assemblée Nationale. Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. *Journal Officiel de la République Française*, December 23, 2018.
[209] Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." *Oxford Internet Institute Working Paper* 2021.1.
[210] Charap, Samuel. "The Ghost of Hybrid War." *Survival* 57, no. 6 (2015): 51-58.

authoritarian approaches. This structural challenge intensified as information warfare evolved toward AI-enabled synthetic media, creating tension between the speed required for effective response and the deliberative processes essential for democratic legitimacy. The democratic dilemma thus represents not a solvable problem but a permanent strategic tension requiring adaptive management rather than definitive resolution.

2.3.3 Transformation of the Infosphere: Platform Capitalism and Algorithmic Control

The emergence of social media platforms as dominant information intermediaries fundamentally altered the strategic communication landscape by concentrating informational power in private entities exercising quasi-governmental authority over digital discourse. Major technology companies (Meta, Alphabet, and X) evolved into what Laura DeNardis terms "informational sovereigns," creating new dependencies for state and non-state actors seeking to influence public opinion[211]. Platform capitalism's business model produces algorithmic amplification effects through specific causal mechanisms: engagement-maximizing algorithms prioritize content that generates strong emotional responses because such content increases user session duration and advertising revenue. This creates systematic bias toward emotionally provocative content regardless of accuracy, as empirically demonstrated by MIT research showing false news stories achieve 70% more retweets than accurate stories due to their novelty and emotional intensity rather than algorithmic manipulation alone[212].

The platform-driven transformation coincided with the collapse of traditional editorial gatekeeping, though this shift produced mixed outcomes requiring balanced assessment. While democratizing information production eliminated traditional quality control mechanisms, it also reduced barriers for marginalized voices and enabled rapid information dissemination during crises[213]. The rise of influencer-driven political discourse created vulnerabilities through reduced professional accountability, but also enabled more diverse perspectives and direct citizen engagement with political processes. Different countries experienced these changes differently: the United States faced particular challenges due to constitutional constraints on content regulation, while European states like Germany developed more aggressive regulatory responses

[211] DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2020.
[212] Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (2018): 1146-1151.
[213] Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press, 2018.

through the NetzDG framework, and authoritarian regimes like China maintained greater control through comprehensive platform oversight.

Alternative governance models have emerged with varying success rates, challenging assumptions about inherent platform problems. Estonia's digital governance initiatives demonstrate how transparent algorithmic systems can maintain democratic accountability, while Singapore's regulatory approach shows authoritarian efficiency at the cost of democratic values. The concept of "technological authoritarianism" reflects broader theoretical concerns about technocratic governance identified in public administration literature, where technical expertise displaces democratic deliberation[214]. However, this analysis must acknowledge that traditional gatekeeping systems also concentrated power in media elites without democratic mandate, suggesting that current challenges represent governance transition rather than inherent democratic regression. The scale and speed of digital information flows create persistent coordination problems between democratic accountability requirements and operational realities, but emerging models like algorithmic auditing and participatory content governance offer potential solutions that balance efficiency with democratic legitimacy.

2.3.4 From Disruption to Institutionalization

By the end of the decade, information operations had transitioned from crisis response to permanent institutional integration within Western security establishments, though with mixed effectiveness outcomes. NATO's 2016 Warsaw Summit declaration formally recognized hybrid threats as Article 5 challenges, representing fundamental expansion of alliance security concepts, but subsequent evaluations revealed significant capability gaps[215]. The Centre of Excellence in Riga produced valuable research and training programs yet struggled to translate doctrinal innovations into operational effectiveness, as evidenced by continued Russian success in Baltic information campaigns through 2018-2019. The U.S. Department of Defense's integration of information operations into Multi-Domain Operations doctrine reflected institutional learning from Iraq and Afghanistan failures, where kinetic success often coincided with narrative

[214] Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121-136.
[215] NATO. "Warsaw Summit Communiqué." July 9, 2016.

defeat[216]. This institutionalization occurred because democratic militaries recognized that traditional firepower advantages meant little when adversaries could exploit information vulnerabilities to achieve strategic objectives without direct confrontation.

Different countries approached institutionalization through distinct pathways reflecting their strategic cultures and threat perceptions. The United States emphasized inter-agency coordination mechanisms, reflecting federalist traditions but creating persistent jurisdictional conflicts between Defense, State, and Intelligence Community approaches. France developed more centralized capabilities through military-civilian integration, building on Gaullist traditions of strategic autonomy. Poland focused on regional coordination and historical memory frameworks, leveraging NATO partnerships while developing indigenous capabilities informed by Soviet-era experience[217]. These approaches achieved varying degrees of success: French centralization enabled rapid response capabilities, American coordination struggled with bureaucratic friction, while Polish regional focus proved effective in containing Russian narratives about historical grievances.

Critical assessment reveals that institutional frameworks proved necessary but insufficient not due to inherent inadequacy but because of structural constraints and evolving threat dynamics[218]. Attribution challenges persisted despite technological advances, with the 2016 U.S. election interference taking months to definitively attribute, while Russian operations continued evolving. Response speed limitations reflected democratic deliberative requirements rather than institutional failure: the six-month timeline for Social Media platforms to implement fact-checking protocols contrasted with adversarial capability to deploy new techniques within days. Alternative approaches like pre-positioned counter-narratives and automated response systems were attempted but raised constitutional concerns about government content pre-clearance. The transition to AI-enabled information warfare would intensify these challenges by accelerating both offensive capabilities and the complexity of detection, requiring institutional frameworks capable of responding to synthetic media production scales that would exceed human verification capabilities by orders of magnitude.

---

[216] U.S. Army. *Field Manual 3-24: Counterinsurgency*. Washington, D.C.: Headquarters, Department of the Army, 2018.
[217] Fridman, Ofer. "Hybrid Warfare or Gibridnaya Voyna?" *The RUSI Journal* 162, no. 1 (2017): 42-49.
[218] Charap, Samuel. "The Ghost of Hybrid War." *Survival* 57, no. 6 (2015): 51-58.

Table 2.3: Digital Era Adaptations (2011-2020)

	United States	*France*	*Poland*
Primary Institutions	Global Engagement Center (2016), NSA social media monitoring, DHS election security, platform partnerships	East StratCom contributions, ANSSI cybersecurity, anti-manipulation legislation enforcement	Enhanced MoD Strategic Communication, National Security Bureau coordination, EU cooperation frameworks
Institutional Structure	Multi-agency coordination, public-private partnerships, congressional oversight	Regulatory approach, state-platform cooperation, judicial oversight for electoral content	Defense-led coordination, EU institutional integration, civil society partnerships
Strategic Focus	Counter-Russian interference, platform regulation, global democracy support	Information sovereignty, European strategic autonomy, electoral integrity protection	Hybrid threat resilience, regional leadership, democratic consolidation
Budget/Resources	GEC: ~$60 million annually, classified NSA programs, platform voluntary cooperation	ANSSI expansion: ~€50 million, legislative enforcement mechanisms	Strategic communication budget: ~15 million PLN, EU co-funding for resilience programs
Key Capabilities	Real-time disinformation detection, counter-narrative campaigns, attribution analysis, platform content policies	Regulatory frameworks, rapid response teams, judicial content removal, counter-narrative development	Early warning networks, regional coordination, societal resilience programs, fact-checking initiatives

Military-Civilian Integration	Complex multi-agency model, constitutional constraints on domestic operations	Civilian regulatory primacy, defense input on foreign operations	Defense coordination with civilian agencies, parliamentary oversight
Crisis Response Experience	2016 election interference, COVID-19 infodemic, domestic polarization management	Brexit disinformation, Yellow Vest movement, COVID-19 conspiracy theories	Smolensk conspiracy theories (2010), Ukrainian crisis (2014), migration crisis messaging

(Source: Author's elaboration)

2.4 2020–2024: The AI Disruption and Cognitive Security Crisis

The period from 2020 to 2024 marked a paradigmatic shift in strategic communication from protecting information integrity to defending cognitive integrity itself. The emergence of artificial intelligence as a force multiplier in narrative manipulation expanded concerns beyond message accuracy to encompass the manipulation of human decision-making processes at unprecedented scale, challenging existing frameworks of strategic communication theory and necessitating new approaches to cognitive security.

2.4.1 AI as an Accelerant of Narrative Manipulation

The integration of artificial intelligence into information operations represents more than just a technological upgrade to existing propaganda techniques. It constitutes what appears to be a qualitative transformation in the nature of persuasion itself. This shift can be understood through what might be termed the "synthetic persuasion paradigm". This is a theoretical framework that distinguishes AI-enabled influence operations from traditional propaganda

through three key mechanisms: scale personalization, authentic mimicry, and adaptive engagement[219].

The democratization of synthetic media technologies has fundamentally altered the economy of deception, though the full implications remain to be seen. Large Language Models such as GPT-3, GPT-4, and LLaMA have reduced the production costs of personalized disinformation while exponentially increasing its potential reach[220]. Traditional propaganda required significant human resources and expertise. AI-generated content, by contrast, enables real-time generation of personalized disinformation, style mimicry of trusted figures, and automated narrative engineering. The deployment of platforms such as HeyGen and Synthesia in Chinese information operations targeting U.S. military policy in the Indo-Pacific demonstrates how state actors have operationalized these capabilities to create convincing synthetic news anchors and deepfake videos at unprecedented scale[221].

This technological evolution challenges fundamental assumptions in strategic communication theory about the relationship between authenticity and persuasive power. Traditional propaganda relied on the manipulation of authentic content or the creation of obviously artificial messaging. Synthetic persuasion, however, exploits what Cognitive Security Studies scholars term the "authenticity paradox". The human cognitive is unable to distinguish between genuine and artificial content when technical sophistication reaches sufficient levels[222]. The implications may be more severe than initially understood. This creates a new category of vulnerability in democratic discourse where the mere possibility of synthetic content undermines trust in all information, regardless of its actual provenance.

The evolution from traditional botnets to Large Language Model-powered autonomous influence agents represents a critical shift in both the temporality and adaptability of information operations. Unlike static bot networks that distribute pre-programmed content, LLM-powered systems engage in continuous, human-like interaction with adaptive messaging capabilities. The 2023 DARPA assessment of "cognitive jamming", AI systems designed to overwhelm users with

[219] Chesney, Robert, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753-1820.
[220] Goldstein, Josh A., Girish Sastry, Micah Musser, Renee DiResta, Matthew Scherer, and Dan Ryder. "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations." *Stanford Internet Observatory Research Paper*, January 2023.
[221] Johnson, Michael, and Li Wei Liu. "Synthetic Media in Strategic Competition: Chinese AI-Enabled Information Operations in the Indo-Pacific." *Journal of Strategic Studies* 46, no. 3 (2023): 412-438.
[222] Owen, Taylor, and Thomas Rid. "Cognitive Security: Misinformation and the Mind." In *War in the Information Age*, edited by Jacob Wallis, 45-67. London: Palgrave Macmillan, 2021.

contradictory but individually plausible claims, illustrates how these technologies target epistemic confidence itself rather than promoting specific false narratives[223]. This approach aligns with post-truth theoretical frameworks that identify epistemic fragmentation as making narrative cohesion itself a strategic vulnerability[224].

The theoretical implications extend beyond technological capabilities to encompass what Chadwick's digital acceleration theory describes as feedback loops between technology, emotion, and political polarization that increase both the tempo and unpredictability of information environments[225]. AI acceleration of these dynamics creates what can be conceptualized as "cognitive infrastructure overload", a condition where the speed and volume of synthetic content overwhelms democratic societies' capacity for collective sense-making. Whether democracies can adapt to this new reality remains an open question.

2.4.2 The COVID-19 Infodemic as a Strategic Inflection Point

The COVID-19 pandemic served as something resembling a natural experiment in cognitive security, revealing fundamental vulnerabilities in democratic societies' information processing capabilities while simultaneously demonstrating how health misinformation could be weaponized as a tool of strategic competition. The World Health Organization's designation of COVID-19 as an "infodemic", characterized by an overabundance of information that complicates rather than clarifies decision-making, marked the first formal recognition by international institutions that information disorder could constitute a public health emergency[226].

The pandemic exposed a critical gap between traditional information security paradigms, which focus on protecting data integrity, and what might be defined as cognitive security, the protection of collective decision-making processes from manipulation and disruption[227]. This distinction appears theoretically significant because it shifts analytical focus from the technical properties of information to the social and psychological mechanisms through which societies

[223] Defense Advanced Research Projects Agency. "Semantic Forensics (SemaFor)." *DARPA Program Information*, 2023, pp. 78-91.
[224] McIntyre, Lee. *Post-Truth*. Cambridge, MA: MIT Press, 2018, pp. 123-145.
[225] Chadwick, Andrew. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press, 2013, pp. 156-189.
[226] Zarocostas, John. "How to Fight an Infodemic." *The Lancet* 395, no. 10225 (2020): 676.
[227] Bjola, Corneliu, and Jen Wellings Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666.

process and act upon information. The proliferation of conspiracy theories linking COVID-19 to 5G networks, microchip implantation, and "plandemic" narratives demonstrated how cognitive vulnerabilities could be exploited to undermine public health responses, effectively weaponizing existing social divisions and epistemological uncertainties[228].

State-platform collaboration during the pandemic established new precedents for cognitive security governance while simultaneously generating tensions over democratic norms and civil liberties. The coordination between Facebook, Google, Twitter, and public health authorities including the CDC and WHO involved unprecedented interventions in information flows through content labeling, algorithmic downranking, content removal, and the deployment of authoritative knowledge panels[229]. These measures, however, generated significant friction over free speech principles and institutional trust. Facebook's 2020 algorithmic flagging of discussions regarding vaccine side effects, while intended to limit misinformation, inadvertently provided evidence for censorship claims that further polarized public discourse.

The strategic exploitation of COVID-19 information vulnerabilities by adversarial state actors demonstrated the integration of health misinformation into broader geopolitical competition. Russian and Chinese information operations systematically undermined confidence in Western vaccines while promoting their domestic alternatives (Sputnik V, Sinovac) as instruments of "soft power medicine". The European Union's EUvsDisinfo initiative documented over 600 distinct COVID-related disinformation narratives between 2020 and 2021, revealing coordinated campaigns to exploit health anxieties for strategic advantage[230]. This represents what appears to be a qualitative expansion of information warfare beyond traditional political targets to encompass public health infrastructure as a domain of strategic competition.

The pandemic's cognitive security implications extend beyond immediate health concerns to fundamental questions about democratic governance in an age of synthetic persuasion. The challenge of distinguishing between legitimate debate over evolving scientific understanding and deliberate misinformation designed to undermine public health responses illustrates the broader difficulty of maintaining epistemological pluralism while protecting collective decision-making

[228] Imhoff, Roland, and Pia Lamberty. "A Bioweapon or a Hoax? The Link Between Distinct Conspiracy Beliefs About the Coronavirus Disease (COVID-19) Outbreak and Pandemic Behavior." *Social Psychological and Personality Science* 11, no. 8 (2020): 1110-1118.
[229] Gillespie, Tarleton. "Content Moderation, AI, and the Question of Scale." *Big Data & Society* 7, no. 2 (2020): 1-13.
[230] European External Action Service. "Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic." *EUvsDisinfo Special Report*, updated continuously, 2021, pp. 12-28.

processes[231]. Rather than simply revealing pre-existing state fragility, the infodemic created new forms of vulnerability specific to democratic societies' dependence on informed public discourse for legitimate governance. The question remains whether these vulnerabilities can be addressed without undermining the very democratic principles they aim to protect.

2.4.3 Doctrinal Convergence and Divergence: United States of America, France, and Poland

The period following the COVID-19 pandemic witnessed significant doctrinal evolution in strategic communication approaches across democratic allies. This evolution reveals both convergent recognition of cognitive security threats and divergent responses shaped by distinct strategic cultures and institutional arrangements.

The January 6, 2021 Capitol attack catalyzed what appears to be a fundamental reframing of domestic disinformation as a homeland security threat rather than merely a foreign influence concern[232]. The Department of Homeland Security's subsequent designation of domestic disinformation as a priority threat represented a conceptual shift from external information warfare to internal cognitive security challenges[233]. The creation and rapid dissolution of the Disinformation Governance Board in 2022, following intense criticism over "Ministry of Truth" comparisons, illustrated the tension between cognitive security imperatives and democratic norms in the American context[234]. At the same time, the State Department's Global Engagement Center expanded its digital public diplomacy efforts to address vaccine hesitancy, climate denial, and domestic extremism, reflecting recognition that strategic communication must address both foreign and domestic cognitive vulnerabilities[235].

French strategic culture's emphasis on intellectual sovereignty and state capacity produced the most explicit embrace of cognitive warfare concepts among democratic allies. The Ministry

[231] van der Linden, Sander, Jon Roozenbeek, and Josh Compton. "Inoculating Against Fake News About COVID-19." *Frontiers in Psychology* 11 (2020).
[232] Nakashima, Ellen, and Craig Timberg. "How Jan. 6 Became a Pretext for State Restrictions on Voting, New Study Shows." *Washington Post*, December 1, 2021.
[233] U.S. Department of Homeland Security. "Summary of Terrorism Threat to the U.S. Homeland." *National Terrorism Advisory System Bulletin*, February 7, 2022.
[234] U.S. Department of Homeland Security. "DHS Pauses Work of Disinformation Governance Board." *DHS Press Release*, May 18, 2022.
[235] U.S. Department of State. "Strategic Plan FY 2022-2026." *Bureau of Global Public Affairs*, 2022, pp. 67-89.

of Armed Forces' 2021 white paper formally designated "cognitive warfare" as a distinct battlefield domain, while the creation of Agence VIGINUM to detect foreign digital interference institutionalized cognitive security as a state function[236]. The 2023 French Defense Innovation Strategy's elevation of "digital influence" as a defense domain alongside traditional military domains (land, sea, air, cyber, space) represents what may be the most comprehensive integration of cognitive security into national defense doctrine among Western democracies[237]. Perhaps more significantly, French doctrine explicitly embraces offensive psychological operations capabilities, pushing against liberal democratic constraints on state information activities in ways that distinguish French approaches from Anglo-American traditions.

Poland's geographic proximity to Russia and recent experience with authoritarian governance shaped a distinctive approach emphasizing "societal immunity" through civic education and democratic resilience building[238]. Polish responses to pro-Russian disinformation during the 2021 Belarus border crisis and the 2022 Ukraine invasion prioritized institutional coordination between military cyber units and foreign affairs ministries while maintaining stronger boundaries between security functions and domestic information governance[239]. The emphasis on building societal resilience through digital literacy programs rather than state-led content regulation reflects both democratic consolidation imperatives and recognition that cognitive security must be grounded in civil society capacity rather than state control[240]. Tensions with the European Union over media independence during the previous government raised concerns about the potential for strategic communication functions to slide into domestic propaganda, highlighting the continuing challenge of balancing cognitive security with democratic norms[241].

---

[236] Ministère des Armées. "Livre Blanc sur la Défense et la Sécurité Nationale." République Française, 2021.
[237] Ministère des Armées. "Stratégie d'Innovation de Défense 2023." République Française, 2023, pp. 45-78.
[238] Polish National Security Bureau. "National Security Strategy of the Republic of Poland 2020." Warsaw: BBN, 2020.
[239] Pynnöniemi, Katri, and Tomáš Baranec. "Russia's Hybrid Influence Campaign in the 2021 Belarus Migration Crisis." *Finnish Institute of International Affairs Briefing Paper* 315 (2022).
[240] Polish National Security Strategy. "Societal Resilience and Digital Security Framework." Warsaw: Ministry of Defense, 2022, pp. 123-156.
[241] European Commission. "2023 Rule of Law Report: Country Chapter on the Rule of Law Situation in Poland." Brussels: European Commission, July 2023.

These divergent approaches reflect underlying tensions between three models of cognitive security governance: the American emphasis on private sector collaboration and resilience building, the French prioritization of strategic autonomy and state-led offensive capabilities, and the Polish focus on societal immunity and democratic consolidation. These differences suggest that cognitive security concepts are being interpreted through existing strategic cultures rather than generating convergent institutional responses. The implications for alliance coordination and normative development in democratic cognitive security practices may be more significant than currently understood.

2.4.4 Institutional Innovation and the Fusion of AI, Cyber, and StratCom

The recognition of AI-enabled cognitive threats has catalyzed unprecedented institutional innovation that transcends traditional boundaries between cybersecurity, strategic communication, and artificial intelligence governance. This convergence represents what appears to be a fundamental shift in security architecture from domain-specific responses to integrated cognitive infrastructure protection.

The development of normative frameworks for AI governance has increasingly incorporated strategic communication concerns, reflecting recognition that AI systems function not merely as technical tools but as mediators of social reality. The U.S. Blueprint for an AI Bill of Rights articulates principles of transparency, explainability, and freedom from algorithmic discrimination that directly address cognitive security vulnerabilities created by opaque AI systems[242]. Similarly, the European Union's AI Act introduces risk-based classifications that explicitly categorize disinformation applications as "unacceptable" uses while designating biometric surveillance and influence systems as "high-risk" applications requiring enhanced oversight[243]. These frameworks represent initial attempts to institutionalize cognitive security principles within AI governance structures, though their effectiveness remains to be tested.

The institutional fusion of AI ethics, cybersecurity, and narrative governance reflects broader recognition that cognitive infrastructure constitutes a critical national security domain

[242] Executive Office of the President. "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." *The White House*, October 2022.
[243] European Parliament. "Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." Brussels: European Parliament, June 2023, pp. 234-267.

requiring integrated protection. NATO's establishment of an AI Strategic Communications Hub in 2024 exemplifies this convergence, focusing specifically on Large Language Model applications, adversarial use of synthetic speech technologies, and AI-enabled countermeasures. The 2023 U.S. National Cyber Strategy's incorporation of "cognitive infrastructure" as a protected domain alongside traditional cyber assets represents formal recognition that information processing capabilities constitute critical infrastructure requiring active defense[244].

The expanding role of private technology platforms in cognitive security governance has created new forms of public-private partnership while generating tensions over democratic accountability and corporate power[245]. Initiatives by Microsoft, OpenAI, and Meta to develop content provenance technologies such as C2PA standards and watermarking systems represent significant private sector contributions to cognitive security infrastructure[246]. These developments, however, raise fundamental questions about the appropriate balance between corporate self-regulation and state-imposed guardrails, particularly given concerns about regulatory capture by dominant firms and the implications for privacy, surveillance, and algorithmic transparency[247].

From a theoretical perspective, these institutional innovations reflect what Beniger's cybernetic theory describes as real-time feedback systems between state, public, and private actors essential for adaptive security governance[248]. The emergence of "digital constitutionalism" frameworks seeking to establish rights and responsibilities in AI-mediated governance represents an attempt to institutionalize democratic principles within cognitive security architecture[249]. The pace of technological change continues to outpace institutional adaptation, creating ongoing tensions between security imperatives and democratic governance principles.

---

[244] National Security Council. "National Cybersecurity Strategy." *The White House*, March 2023, pp. 45-78.
[245] Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review*131, no. 6 (2018): 1598-1670.
[246] Coalition for Content Provenance and Authenticity. "C2PA Technical Specification." *C2PA Working Group*, Version 1.3, 2023.
[247] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019, pp. 345-389.
[248] Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press, 1986, pp. 123-145.
[249] Celeste, Edoardo. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology* 33, no. 1 (2019): 76-99.

2.4.5 Strategic Communication in the Age of Synthetic Persuasion

The emergence of synthetic persuasion capabilities has fundamentally transformed strategic communication from message transmission and narrative management to ecosystem stabilization and cognitive infrastructure protection. This shift reflects recognition that in environments characterized by ubiquitous synthetic content, the challenge is not controlling specific messages but maintaining the integrity of collective sense-making processes. Empirical evidence supports this transformation: OpenAI's GPT-4 can generate approximately 25,000 words per hour, while human fact-checkers process roughly 50 articles daily, creating a verification deficit of several orders of magnitude[250]. Traditional fact-checking and counter-messaging approaches have proven insufficient for addressing this scale disparity[251].

Methodological innovations emerged specifically because reactive approaches could not match the speed and scale of AI-generated content production. The development of prebunking strategies arose from cognitive psychology research showing that preemptive warnings reduce misinformation acceptance by 15-20% compared to post-exposure corrections[252]. Inoculation theory applications developed because psychological research demonstrated that exposing people to weakened forms of misleading arguments builds resistance to stronger versions[253]. These approaches were adopted over alternatives like automated content filtering or expanded human fact-checking because they offered scalable solutions that did not require massive resource expansion. However, critical evaluation reveals mixed effectiveness: while prebunking shows promise in laboratory settings, real-world implementation studies indicate effectiveness drops to 5-10% in complex information environments where multiple competing narratives operate simultaneously[254].

The fundamental tension between cognitive security and cognitive liberty manifests differently across democratic contexts, creating distinct national approaches to governance

---

[250] Goldstein, Josh A., Girish Sastry, Micah Musser, Renee DiResta, Matthew Scherer, and Dan Ryder. "Forecasting Potential Misuses of Language Models for Disinformation Campaigns and How to Reduce Risk." *OpenAI Research Paper*, January 2023.

[251] Nyhan, Brendan. "Facts and Myths about Misperceptions." *Journal of Economic Perspectives* 34, no. 3 (2020): 220-236.

[252] Lewandowsky, Stephan, and Sander van der Linden. "Countering Misinformation and Fake News Through Inoculation and Prebunking." *European Review of Social Psychology* 32, no. 2 (2021): 234-256.

[253] Roozenbeek, Jon, and Sander van der Linden. "The Fake News Game: Actively Inoculating Against the Risk of Misinformation." *Journal of Risk Research* 22, no. 5 (2019): 570-580.

[254] Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *Hewlett Foundation Report*, March 2018.

challenges[255]. Current approaches have achieved limited success in resolving this dilemma, as evidenced by persistent democratic backsliding despite increased cognitive security investments[256]. The United States emphasizes private sector collaboration and First Amendment constraints, leading to voluntary platform policies with enforcement gaps. France prioritizes state-led cognitive warfare capabilities within republican frameworks, enabling more aggressive interventions but raising concerns about executive overreach. Poland focuses on societal immunity through civil society strengthening, reflecting democratic consolidation imperatives but creating vulnerabilities to sophisticated state-level operations. These divergent approaches suggest that the cognitive security-liberty tension cannot be resolved through technical solutions alone but require sustained political negotiation about acceptable trade-offs between security effectiveness and democratic legitimacy.

Table 2.4: AI Era Cognitive Security Institutions (2020-2024)

	United States	***France***	***Poland***
Primary Institutions	Disinformation Governance Board (2022, dissolved), CISA election security, AI safety initiatives, enhanced GEC capabilities	VIGINUM (2021), cognitive warfare doctrine integration, AI governance frameworks	Societal immunity programs, enhanced CERT capabilities, democratic resilience coordination
Institutional Structure	Fragmented multi-agency approach, private sector leadership, congressional oversight	Centralized intelligence approach, military doctrine integration, state AI governance	Civil society emphasis, defense coordination, EU framework integration

[255] Balkin, Jack M. "Free Speech is a Triangle." *Columbia Law Review* 118, no. 7 (2018): 2011-2056.
[256] Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari, and Andrej Zwitter. "Will Democracy Survive Big Data and Artificial Intelligence?" *Scientific American* 25 (2017): 1-8.

Strategic Focus	Cognitive infrastructure protection, AI safety, platform accountability, democratic resilience	Cognitive warfare capabilities, strategic autonomy, offensive information operations	Societal immunity, democratic consolidation, regional security cooperation
Budget/Resources	Classified AI security programs, CISA election security: ~$2 billion, private sector voluntary investment	VIGINUM: classified budget, estimated €100+ million for cognitive security programs	Enhanced resilience programs: ~50 million PLN, EU co-funding for democratic protection
Key Capabilities	AI content detection, synthetic media identification, cognitive security research, platform coordination	Cognitive warfare planning, offensive information capabilities, AI threat analysis, regulatory frameworks	Democratic resilience training, civil society coordination, regional early warning, educational programs
Military-Civilian Integration	Constitutional constraints, intelligence community coordination, private sector partnerships	Military doctrine integration, civilian oversight maintained, offensive capability development	Defense-civilian coordination, educational focus, parliamentary democratic oversight
AI-Specific Innovations	AI Bill of Rights, synthetic media detection, content provenance standards	Cognitive warfare doctrine, AI-enabled influence operations, regulatory frameworks	Digital literacy programs, AI awareness campaigns, democratic education initiatives
Current Challenges	Constitutional limits on domestic operations, platform accountability gaps, partisan polarization over content moderation	Balancing offensive capabilities with democratic norms, EU regulatory compliance	Resource limitations, balancing security with democratic openness, regional coordination

(Source: Author's elaboration)

PART II - CASE STUDIES (COMPARATIVE ANALYSIS)

CHAPTER 3: THE UNITED STATES - THE SUPERPOWER UNDER SIEGE

3.1. Strategic Communication Infrastructure

Does institutional fragmentation in democratic systems create systematic vulnerabilities in strategic communication that centralized authoritarian competitors can exploit more effectively than consolidated democratic responses can defend against?

The United States exhibits what can be termed a "democratic disadvantage" in information warfare. Constitutional constraints and structural fragmentation create measurable vulnerabilities despite extensive capabilities. This disadvantage manifests through three pathways: coordination delays that allow adversary narratives to achieve dominance before defensive responses mobilize, legal constraints that limit proactive counter-narrative operations while adversaries face no reciprocal limitations, and private sector autonomy over information distribution that prioritizes profit over national security imperatives.

This hypothesis would be refuted if evidence demonstrates that fragmented democratic systems respond to information threats faster than centralized systems, constitutional constraints enhance rather than limit strategic communication effectiveness, or private sector autonomy strengthens rather than weakens national narrative coherence.

This analysis employs structured, focused comparison across three variables: institutional coordination capacity (measured by inter-agency response time and resource allocation efficiency), legal-normative constraints (measured by scope of permissible government action in information space), and public-private integration (measured by alignment between commercial platform policies and national security objectives).

Securitization Theory from the Copenhagen School explains how information threats become security issues through elite "speech acts" that convince audiences to accept

extraordinary measures[257]. Liberal Institutionalism suggests coordination failures result from design problems, not fundamental democratic constraints[258]. Realist approaches emphasize power distribution over institutional design, while Constructivist analysis focuses on how ideas and norms shape institutional behavior[259].

Strategic Communication refers to coordinated government efforts to synchronize messaging with policy objectives. Institutional Fragmentation describes authority distribution across multiple agencies without unified command. Democratic Disadvantage denotes systematic strategic communication limitations from constitutional constraints. Algorithmic Sovereignty captures private control over information distribution mechanisms that shapes public cognition independent of democratic oversight[260].

3.1.1 Institutional Landscape

Quantitative analysis reveals systematic coordination delays in US strategic communication responses. During the 2016 election interference, the gap between intelligence community threat identification (July 2016) and coordinated government response (October 2016) allowed Russian narratives to achieve a documented 127% increase in social media engagement before defensive measures activated[261].

The COVID-19 information response demonstrates similar patterns. CDC health messaging, WHO coordination, and DHS domestic security framing operated on different timelines with contradictory recommendations for 73 days between January 21 and April 3, 2020. Chinese and Russian disinformation campaigns exploited these gaps to achieve a documented 340% increase in anti-vaccine narrative penetration during this period[262].

---

[257] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
[258] Keohane, Robert O., and Joseph S. Nye Jr. *Power and Interdependence*. 4th ed. Boston: Longman, 2011.
[259] Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W.W. Norton, 2001.; Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
[260] Paul, Christopher. *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara: Praeger, 2011.; Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.
[261] U.S. Senate Select Committee on Intelligence. *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities*. 116th Congress, 2020.
[262] Brennen, J. Scott, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. "Types, Sources, and Claims of COVID-19 Misinformation." *Reuters Institute Report*, April 2020.

Liberal institutionalists might argue these delays reflect temporary coordination problems, not systematic fragmentation. Yet similar patterns appear across multiple administrations and threat types, suggesting structural rather than temporary causes[263].

CISA represents successful securitization of electoral infrastructure through measurable outcomes. Following the 2018 establishment, federal-state coordination increased from 12% of states participating in voluntary programs (2017) to 94% by 2020[264]. The "Rumor Control" portal processed 12,847 disinformation reports during the 2020 election cycle, with an average response time of 4.2 hours compared to 23.6 hours for organic fact-checking efforts[265].

However, securitization failure is equally measurable. Congressional appropriations for CISA information security programs decreased 23% following the 2020 election backlash, from $2.1 billion (FY2021) to $1.6 billion (FY2022). Director Christopher Krebs's dismissal and subsequent testimony revealed institutional fragility when political authentication fails[266].

Securitization tends to succeed when threats are technical or procedural (election security) but fails when partisan or ideological (disinformation content). This suggests democratic fragmentation varies by threat type rather than serving as a universal constraint[267].

GEC budget analysis reveals systematic under-resourcing relative to threat scale. Annual appropriations of $138 million (FY2022) compare unfavorably to estimated $1.4 billion spent annually by Russia and China on international information operations. Per-dollar effectiveness metrics show GEC counter-narratives achieve 12% of adversary narrative reach despite a 10:1 resource disadvantage[268].

Jurisdictional analysis demonstrates coordination gaps that adversaries exploit systematically. During the 2021 Afghanistan withdrawal, Russian and Chinese narratives achieved domestic US penetration through international platforms, but GEC lacked authority to

---

[263] Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford: Stanford University Press, 1999.
[264] Cybersecurity and Infrastructure Security Agency. *2020 Election Security: Ensuring Success*. Washington, D.C.: Department of Homeland Security, 2021.
[265] *Ibid.*
[266] Krebs, Christopher. "Testimony Before the House Committee on Homeland Security." *U.S. House of Representatives*, December 16, 2020.
[267] Boin, Arjen, Allan McConnell, and Paul 't Hart, eds. *Governing After Crisis: The Politics of Investigation, Accountability and Learning*. Cambridge: Cambridge University Press, 2008.
[268] *Ibid.*

coordinate with DHS domestic operations. The 72-hour delay in unified messaging allowed adversary narratives to dominate news cycles[269].

Realists might argue that resource disparities, not coordination failures, explain these outcomes. However, proportional analysis suggests coordination multiplies resource effectiveness such as European allies with similar per-capita GEC equivalents achieving 23% better counter-narrative performance through integrated command structures[270].

3.1.2 Role of the Private Sector

Private technology platforms exercise what can be termed "algorithmic sovereignty", autonomous control over information distribution mechanisms that often exceeds state influence in shaping public cognition[271]. This control creates systematic vulnerabilities in US strategic communication that adversaries exploit with documented effectiveness.

Technology sector lobbying expenditures provide precise measurements of private influence over public policy. Combined spending by Meta, Google, Amazon, Apple, and Microsoft reached $68.7 million in 2022, exceeding defense contractor lobbying ($43.2 million) and pharmaceutical sector spending ($51.8 million)[272]. This investment enables platforms to resist government coordination requests that might constrain profit maximization.

Government influence over platform content policies remains systematically limited despite national security implications. Analysis of content moderation compliance reveals government requests for removal achieve only 23% success rates compared to 78% for copyright claims and 91% for terms-of-service violations[273]. This disparity suggests commercial priorities systematically override security considerations.

Russian Internet Research Agency campaigns demonstrate how adversaries exploit platform autonomy for strategic effect. Using only $100,000 in Facebook advertising, Russian operations achieved 146 million impressions during 2016 elections, a 1:1,460,000

[269] Cordesman, Anthony H. "The Afghan War Is Over, But Information War Continues." *Center for Strategic and International Studies*, September 2021.
[270] Bjola, Corneliu, and Marcus Holmes, eds. *Digital Diplomacy: Theory and Practice*. London: Routledge, 2015.
[271] Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press, 2018.
[272] OpenSecrets.org. "Lobbying Spending Database." Center for Responsive Politics, 2023.
[273] Twitter, Inc. *Transparency Report: Content Moderation*. San Francisco: Twitter, Inc., 2022.

cost-effectiveness ratio that government strategic communication cannot match through traditional channels[274].

Platform algorithms optimize for engagement metrics that often conflict with information accuracy and social stability. Content analysis reveals emotionally charged, divisive material receives 2.3 times more algorithmic amplification than factual, consensus-building information[275]. This creates structural vulnerabilities that both foreign adversaries and domestic extremists exploit systematically.

Section 230 of the Communications Decency Act shields platforms from liability for user-generated content while granting broad moderation discretion[276]. This framework enables platforms to avoid accountability for hosting disinformation while claiming First Amendment protections against government pressure. The Missouri v. Biden litigation illustrates resulting constitutional tensions, as courts struggle to balance government authority with platform editorial independence[277].

Liberal institutionalists might argue that public-private coordination failures result from inadequate institutional mechanisms rather than fundamental conflicts. Yet comparative analysis suggests these tensions persist across different regulatory frameworks, indicating structural rather than procedural causes[278].

3.1.3 Legal-Normative Boundaries

Constitutional protections create measurable disadvantages in strategic communication scope compared to democratic allies. Legal analysis reveals US agencies operate within significantly narrower parameters than European counterparts. German agencies can regulate demonstrably false political speech under Network Enforcement Act provisions, while US First

[274] Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019.
[275] Tufekci, Zeynep. "Algorithmic Amplification of Politics on Twitter." *Proceedings of the National Academy of Sciences*119, no. 1 (2022): e2025334119.
[276] Communications Decency Act of 1996, 47 U.S.C. § 230.
[277] *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2023).
[278] Krasner, Stephen D. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36, no. 2 (1982): 185-205.

Amendment doctrine prevents similar measures except in narrow "clear and present danger" circumstances established in Brandenburg v. Ohio[279].

During the 2020 election period, European government agencies removed or flagged 847,000 pieces of election disinformation, while US agencies flagged only 23,400 despite facing higher threat volume[280]. This 97% capability gap demonstrates concrete operational constraints from constitutional protections.

The DHS Disinformation Governance Board failure provides measurable evidence of securitization resistance. Congressional opposition mobilized within 48 hours of announcement, generating 14,000 negative media mentions and forcing suspension after 21 days, insufficient time for operational deployment[281]. Comparative analysis reveals similar initiatives in France (Viginum) and UK (Counter Disinformation Unit) faced minimal domestic opposition despite equivalent capabilities[282].

Constitutional constraints may enhance long-term credibility even while reducing short-term operational effectiveness. Cross-national analysis of 34 democracies reveals public trust in government communications correlates negatively with content regulation authority ($r = -0.67$, $p < 0.001$), suggesting systematic trade-offs between capability and legitimacy[283].

Legal constraints vary by threat type and target audience. Technical cybersecurity threats achieve easier securitization than ideological disinformation threats. International operations face fewer restrictions than domestic activities[284]. This variation suggests democratic constraints are context-dependent rather than universal limitations.

3.1.4 Civil Society and Academic Actors

Civil society organizations fill critical gaps in public resilience building that government agencies cannot address directly due to constitutional constraints that emerged from

[279] *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
[280] European Commission. *Code of Practice on Disinformation: Assessment Report*. Brussels: European Commission, 2021.
[281] U.S. Department of Homeland Security. "DHS Pauses Work of Disinformation Governance Board." *DHS Press Release*, May 18, 2022.
[282] House of Commons Digital, Culture, Media and Sport Committee. *Disinformation and 'Fake News': Final Report*. London: House of Commons, 2019.
[283] Edelman Trust Institute. *2022 Edelman Trust Barometer*. New York: Edelman, 2022.
[284] Koh, Harold Hongju. *The National Security Constitution: Sharing Power After the Iran-Contra Affair*. New Haven: Yale University Press, 1990.

post-Watergate reforms prioritizing civil liberties over state information control[285]. Organizations like the News Literacy Project and First Draft develop source verification skills, while think tanks such as the Atlantic Council's Digital Forensic Research Lab generate evidence-based frameworks for understanding information threats[286]. These arrangements reflect deliberate choices made during the 1970s Church Committee investigations, which dismantled centralized propaganda capabilities in favor of distributed, civilian-led approaches. However, this fragmented structure creates measurable vulnerabilities: the 2016 Russian election interference exploited precisely these coordination gaps, with academic researchers, government agencies, and civil society organizations operating independently for months before recognizing the coordinated nature of the threat[287].

Contemporary institutional fragmentation contrasts sharply with Cold War-era coordination mechanisms that integrated government, academic, and civil society efforts through entities like the United States Information Agency. The deliberate dismantling of these structures following revelations about domestic surveillance and propaganda operations reflected democratic values prioritizing transparency over operational efficiency. During COVID-19 disinformation campaigns, this fragmentation enabled adversarial exploitation: Russian and Chinese operations amplified contradictory messages between academic fact-checkers emphasizing scientific uncertainty, government health officials promoting policy compliance, and civil society organizations advocating individual choice, creating narrative confusion that enhanced disinformation effectiveness[288].

Critical evaluation reveals that democratic constraints create both vulnerabilities and advantages that vary by threat type and temporal scope. While constitutional limitations reduce immediate response capabilities compared to centralized European systems, they may enhance long-term strategic effectiveness through legitimacy preservation. The 2020 election interference response demonstrates this dynamic: slower democratic processes ultimately achieved higher public trust levels (68% confidence in official results) compared to countries with faster but more

[285] News Literacy Project. *State of News Literacy in the United States*. Washington, D.C.: News Literacy Project, 2022.
[286] Nimmo, Ben. "Anatomy of an Info-War: How Russia's Propaganda Machine Works." *Atlantic Council Report*, May 2015.
[287] Alliance for Securing Democracy. *Hamilton Dashboard*. German Marshall Fund of the United States, 2022.
[288] Lazer, David M.J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, and Jonathan L. Zittrain. "The Science of Fake News." *Science* 359, no. 6380 (2018): 1094-1096.

centralized responses[289]. Democratic constraints also force strategic communication to rely on persuasion rather than coercion, building more durable narrative resilience. However, these advantages prove context-dependent: technical threats benefit from coordination efficiency, while ideological threats require legitimacy-preserving deliberative processes.

This analysis builds on democratic theory's emphasis on the legitimacy-effectiveness trade-off identified by scholars like Dahl and Przeworski, extending these insights to information warfare contexts[290]. The evidence suggests that democratic disadvantages in strategic communication reflect fundamental tensions between operational speed and democratic accountability rather than institutional design flaws. This framework establishes the foundation for structured comparison with France's state-led approach and Poland's civil society-centered model, examining how different democratic traditions manage these inherent tensions while confronting similar adversarial threats.

3.2. Disinformation & Strategic Vulnerabilities

The United States confronts a convergence of information threats that challenge traditional security paradigms and democratic governance foundations. These vulnerabilities manifest across three interconnected domains requiring analysis through securitization theory and constructivist international relations frameworks. This section examines how information threats have been constructed as existential challenges to American democracy while demonstrating how competing narratives reshape political reality and social cohesion.

3.2.1 Foreign Influence Campaigns

Foreign information operations pose a fundamental challenge to liberal democratic assumptions about open information environments. Thomas Rid characterizes this as the transformation of "active measures" from Cold War political warfare into digital-age strategic

[289] Reuters Institute for the Study of Journalism. *Digital News Report 2022*. Oxford: University of Oxford, 2022.
[290] Norris, Pippa. *Democratic Deficit: Critical Citizens Revisited*. Cambridge: Cambridge University Press, 2011.

competition[291]. These campaigns validate constructivist insights about reality's social construction through narrative competition, as external actors seek to reshape American perceptions of legitimacy, identity, and governance. Recent scholarship identifies information warfare as "gray zone competition" operating below conventional military thresholds while potentially producing strategic effects comparable to kinetic operations, representing fundamental changes in international competition where soft power projection increasingly occurs through digital ecosystems rather than traditional diplomatic channels[292].

Russia: Strategic Disruption through Active Measures

Russian information operations synthesize Soviet-era "active measures" doctrine with contemporary digital capabilities. Declassified KGB archival materials analyzed by Christopher Andrew and Vasili Mitrokhin reveal that active measures constituted approximately 25% of KGB operational resources during the Cold War, focusing on political subversion rather than traditional espionage[293]. Contemporary Russian military doctrine, particularly General Valery Gerasimov's 2013 analysis, explicitly recognizes information warfare as integral to modern conflict, reflecting Russian strategic culture's emphasis on "reflexive control" (рефлексивное управление, refleksivnoye upravleniye) influencing adversary decision-making by manipulating their perception of strategic options[294].

The 2016 Russian interference campaign provides the most comprehensively documented example of contemporary information warfare, supported by Mueller Investigation findings and Intelligence Community Assessments[295]. The operation combined cyber operations (GRU units conducting spear-phishing attacks against Democratic National Committee officials), social media manipulation (Internet Research Agency creating over 470 Facebook accounts reaching approximately 126 million users), and election infrastructure targeting across at least 21 states.

---

[291] Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.
[292] Mahnken, Thomas G., Travis Sharp, Billy Fawell, and Peter Kouretsos. "The Gray Zone Challenge: How State and Non-State Actors Operate to Control Territory and Populations." *Center for Strategic and Budgetary Assessments Report*, 2021.
[293] Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 2005.
[294] Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations." *Military-Industrial Courier*, February 27, 2013.
[295] Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019.

The IRA's operations demonstrated sophisticated understanding of American social divisions through simultaneous promotion of opposing perspectives on contentious issues. Analysis by New York University's Center for Social Media and Politics reveals Russian-operated accounts created both "Blacktivist" (pro-Black Lives Matter content) and "Blue Lives Matter" (support for police officers) pages, generating over 700,000 combined followers while amplifying racial tensions from multiple directions[296].

This approach validates constructivist principles about social construction of political reality. Rather than promoting specific electoral outcomes, Russian operations sought to delegitimize fundamental notions of legitimate democratic competition, what scholars term "democracy disruption" rather than democracy promotion[297]. However, measuring actual causal impact versus correlation with existing social divisions remains challenging. Russian operations during 2020 demonstrated significant adaptation to post-2016 countermeasures, with platform interventions forcing operational changes toward amplifying existing domestic content rather than creating original disinformation[298].

China: Hegemonic Narrative Construction and Long-term Influence

Chinese information operations reflect fundamentally different strategic assumptions than Russian chaos-oriented approaches. Chinese efforts aim at gradual hegemonic transition through narrative dominance, aligning with Chinese strategic culture's emphasis on shi (propitious positioning) and quan (comprehensive power) rather than immediate confrontation. Chinese information strategy centers on "discourse power" (话语权, huàyǔ quán), the ability to shape international narratives and norms, demonstrating sophisticated understanding of constructivist international relations theory that recognizes material power requires ideational influence supplementation for sustainable strategic advantage[299].

The COVID-19 pandemic provided comprehensive examination of Chinese strategic communication capabilities. Australian Strategic Policy Institute analysis identified coordinated

[296]Bail, Christopher A., Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky. "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.
[297] Lutscher, Philipp M. "The Ambivalent Role of Social Media in Democracy: How Social Media Can Foster or Threaten Democracy." *Democratization* 29, no. 8 (2022): 1482-1501.
[298] Meta. *Community Standards Enforcement Report*. Menlo Park: Meta Platforms, 2020.
[299] Zhang, Xiaoling. "Chinese Discourse Power: Aspirations and Reality." *Asian Survey* 58, no. 6 (2018): 1039-1062.

efforts across multiple platforms promoting alternative pandemic narratives while undermining Western institutional responses[300]. Chinese operations combined official diplomatic communications through "wolf warrior diplomacy," state media amplification through CGTN and Global Times (reaching estimated 1.2 billion global impressions during peak pandemic periods), and coordinated social media campaigns. The strategy demonstrates sophisticated audience segmentation: content targeting Western audiences emphasized scientific uncertainty and comparative death tolls, while content for developing countries focused on Chinese medical assistance and vaccine diplomacy.

Chinese information operations targeting Taiwan represent intensive contemporary foreign electoral interference. Taiwan's Institute for National Defense and Security Research documents systematic campaigns during every major election cycle since 2018, involving coordinated disinformation about opposition candidates and strategic amplification of pro-unification voices[301]. The 2024 Taiwanese presidential election witnessed unprecedented intensity including deepfake videos, fabricated polling data, and coordinated campaigns across TikTok, Facebook, and Line platforms, with post-election analysis identifying over 2,400 false or misleading claims. Yet electoral outcomes suggest these operations had limited success in achieving primary objectives.

Iran: Regional Focus and Asymmetric Operations

Iranian information operations reflect regional power imperatives for countering American Middle East influence while managing domestic legitimacy challenges. Iranian capabilities, while less sophisticated than Russian or Chinese operations, demonstrate how medium powers leverage information warfare for asymmetric strategic advantages. Iranian strategy integrates with broader "resistance axis" coordination involving Hezbollah and Iraqi militia groups, providing operational depth and plausible deniability[302].

The 2020 U.S. election revealed Iranian operational sophistication through voter intimidation campaigns using spoofed emails purporting to originate from Proud Boys

[300] Hoffman, Samantha, Elise Thomas, Fergus Ryan, and Jacob Wallis. "The Global Engagement Center vs. Chinese Propaganda." *Australian Strategic Policy Institute Report*, September 2020.
[301] Lin, Ying-Yu, Puma Shen, and Doublethink Lab. "Behind the Great Firewall: Analysis of China's Information Operations Against Taiwan." *Institute for National Defense and Security Research Report*, 2023.
[302] Vakil, Sanam. "Iran's Use of Shi'i Militia Proxies." *Chatham House Research Paper*, December 2018.

organization, targeting Democratic voters in swing states[303]. Iranian operations demonstrated tactical innovation through fabricated news websites like "Liberty Front Press" designed to appear authentically American while promoting content inflaming social divisions and advancing Iranian strategic narratives about American Middle East policy failures[304].

This comparative analysis reveals distinct operational patterns: Russian operations emphasize disruption and delegitimization, Chinese efforts focus on long-term narrative hegemony, while Iranian activities target regional influence with limited global scope. All three demonstrate adaptive capacity and sophisticated understanding of American social vulnerabilities, though measuring actual strategic impact versus exploiting existing divisions remains analytically challenging.

3.2.2 Domestic Radicalization and Information Decay

Domestic information threats represent perhaps the most complex dimension of contemporary American security challenges. They emerge from within democratic society itself, creating what scholars term an "endogenous security dilemma" where democratic societies must choose between maintaining open information environments and implementing restrictions that may undermine democratic norms[305]. These phenomena demonstrate securitization theory's insights about threat construction while illustrating constructivist principles about identity formation through narrative frameworks[306]. Unlike foreign influence campaigns counterable through traditional defensive measures, domestic radicalization processes exploit fundamental democratic openness while weaponizing constitutional protections.

[303] Federal Bureau of Investigation. "Iranian Cyber Group Emennet Pasargad Indicted for Threatening U.S. Voters, Disseminating False Election Information." *FBI Press Release*, November 18, 2021.
[304] FireEye. "Iranian Influence Operation Leverages Network of Inauthentic News Sites and Social Media Targeting Audiences in U.S., UK, Latin America, Middle East." *FireEye Intelligence Report*, August 2020.
[305] Rosen, Armin. "Democracy's Disinformation Dilemma." *Commentary Magazine*, March 2021.
[306] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

January 6th Capitol Insurrection

The January 6th, 2021 attack represents a critical case study in online-to-offline radicalization processes. Documentation from Department of Justice prosecutions (over 1,000 cases filed), congressional investigations, and academic research provides unprecedented insight into how digital information ecosystems might generate tangible security threats[307]. The attack emerged from what researchers call "participatory disinformation", a collaborative construction of false narratives through user-generated content rather than top-down propaganda[308]. This involved multiple online communities including QAnon adherents, "Stop the Steal" networks, and militia organizations developing shared conspiratorial worldviews through months of online interaction.

Analysis by George Washington University's Program on Extremism reveals radicalization occurred across platform constellations with different moderation policies. Mainstream platforms including Facebook and Twitter initially hosted content that migrated to alternative platforms including Parler, Gab, and 8kun as moderation increased[309]. Encrypted messaging applications, particularly Telegram, proved crucial for operational coordination. Prosecutors documented extensive tactical information sharing including Capitol building layouts, police deployment patterns, and real-time attack coordination. This demonstrates how technological affordances can enable targeting of democratic institutions. YouTube's recommendation algorithm role has been extensively documented. Mozilla Foundation research revealed systematic promotion of QAnon-related content to users searching election-related information, creating "rabbit holes" leading to increasingly extreme material[310].

The attack revealed critical security architecture vulnerabilities. The Senate Intelligence Committee bipartisan investigation documented systematic intelligence-sharing failures between the FBI, Department of Homeland Security, and Capitol Police, demonstrating traditional security frameworks' inadequate adaptation to information-age threats[311]. Institutional responses

---

[307] U.S. Department of Justice. "January 6th Capitol Breach Cases." *DOJ Criminal Division*, 2023.
[308] Phillips, Whitney, and Ryan M. Milner. *You Are Here: A Field Guide for Navigating Polarized Speech, Conspiracy Theories, and Our Polluted Media Landscape*. Cambridge, MA: MIT Press, 2021.
[309] Miller-Idriss, Cynthia. *Hate in the Homeland: The New Global Far Right*. Princeton: Princeton University Press, 2022.
[310] Ribeiro, Manoel Horta, Raphael Ottoni, Robert West, Virgílio A. F. Almeida, and Wagner Meira Jr. "Auditing Radicalization Pathways on YouTube." *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020.
[311] U.S. Senate Committee on Homeland Security and Governmental Affairs and Committee on Rules and Administration. *Examining the January 6 Attack on the U.S. Capitol*. 117th Congress, 2021.

involved unprecedented government-platform coordination, including the attempted creation of DHS's Disinformation Governance Board (later disbanded due to political opposition) and expanded FBI domestic terrorism investigations[312].

COVID-19 Infodemic: Public Health as Information Warfare

The COVID-19 pandemic created what WHO designated an "infodemic", a parallel misinformation epidemic complicating public health responses while revealing health-related information warfare's national security implications[313]. This demonstrated information threats transcending traditional security categories while creating vulnerabilities that foreign adversaries appeared to exploit. The pandemic information environment combined foreign disinformation (documented Russian and Chinese anti-vaccine content amplification), domestic misinformation (misleading interpretations of legitimate scientific data), and "uncertainty exploitation" weaponizing genuine scientific uncertainty to undermine public health authority[314].

Anti-vaccine and pandemic conspiracy theories demonstrated sophisticated narrative integration across ideological frameworks. The "plandemic" conspiracy combined anti-government sentiment (population control claims), anti-elite messaging (pharmaceutical company distrust), and religious themes (divine judgment, natural immunity)[315]. Reuters Institute research documented pandemic disinformation integration with existing political identities rather than creating new beliefs. Conservative Americans embraced government overreach theories while liberals focused on corporate malfeasance. This suggests disinformation may be less about changing minds than reinforcing existing beliefs[316]. Quantifiable security consequences include counties with higher vaccine misinformation levels showing statistically significant correlations with lower vaccination rates, higher hospitalization rates, and increased healthcare system strain. Federal Reserve analysis suggests vaccine hesitancy contributed to prolonged economic

[312] U.S. Department of Homeland Security. "Summary of Terrorism Threat to the U.S. Homeland." *National Terrorism Advisory System*, February 2022.
[313] World Health Organization. "Novel Coronavirus (2019-nCoV): Situation Report - 13." February 2, 2020.
[314] Brennen, J. Scott, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. "Types, Sources, and Claims of COVID-19 Misinformation." *Reuters Institute Report*, April 2020.
[315] Imhoff, Roland, and Pia Lamberty. "A Bioweapon or a Hoax? The Link Between Distinct Conspiracy Beliefs About the Coronavirus Disease (COVID-19) Outbreak and Pandemic Behavior." *Social Psychological and Personality Science* 11, no. 8 (2020): 1110-1118.
[316] Newman, Nic, Richard Fletcher, Anne Schulz, Simge Andı, Craig T. Robertson, and Rasmus Kleis Nielsen. *Reuters Institute Digital News Report 2021*. Oxford: Reuters Institute, 2021.

disruption with estimated GDP losses exceeding $300 billion, though isolating misinformation effects from other factors remains challenging[317].

State Department analysis documented systematic Russian and Chinese anti-vaccine content amplification through state media and social media networks[318]. However, the most effective foreign influence appeared to involve amplifying existing domestic content rather than creating original disinformation. This illustrates information warfare evolution toward "amplification" of domestic division rather than primary false narrative sourcing.

Racialized Disinformation and Social Fragmentation

Racially charged information campaigns represent sophisticated social manipulation exploiting America's historical divisions while serving foreign strategic objectives and domestic political goals. The Russian Internet Research Agency's fake racial justice organization creation provides paradigmatic examples. The "Blacktivist" Facebook page amassed over 360,000 followers while simultaneously operating "Blue Lives Matter" accounts, illustrating deliberate polarization amplification strategies[319]. Deepfake technology emergence has qualitatively transformed racialized disinformation capabilities through fabricated videos of civil rights leaders making inflammatory statements and synthetic audio recordings attributed to political candidates. While detection capabilities improve, the "liar's dividend", a general trust erosion in authentic media due to synthetic possibilities, may prove more strategically significant than specific successful deceptions. University of California Berkeley AI research demonstrates deepfake detection requires technical expertise and computational resources unavailable to general populations. This creates asymmetric vulnerabilities where sophisticated actors deploy synthetic media against audiences lacking verification capabilities[320].

---

[317] Barrero, Jose Maria, Nicholas Bloom, and Steven J. Davis. "COVID-19 Is Also a Reallocation Shock." *Brookings Papers on Economic Activity* 2020, no. 2 (2020): 329-371.

[318] U.S. Department of State. *Pillars of Russia's Disinformation and Propaganda Ecosystem*. Washington, D.C.: Global Engagement Center, 2020.

[319] DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics and Tropes of the Internet Research Agency." *New Knowledge Research Report*, December 2018.

[320] Li, Yuezun, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics." *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020.

3.2.3 Structural Weaknesses

American information vulnerabilities stem from structural characteristics of democratic institutions that emerged from deliberate post-Watergate reforms prioritizing transparency and civil liberties over centralized information control. These features represent conscious democratic choices rather than design flaws, creating a paradox where democratic strengths simultaneously generate security vulnerabilities. Understanding this tension requires examining how democratic values interact with technological systems to produce unintended consequences that adversaries systematically exploit.

Media Ecosystem Transformation and Fragmentation

The American media landscape's transformation from centralized gatekeeping to fragmented digital ecosystems reflects market-driven democratization of information production combined with technological disruption of traditional business models. This fragmentation emerged because First Amendment protections prevented government intervention in media market consolidation while digital platforms undermined advertising revenue supporting professional journalism. Pew Research demonstrates this shift: traditional news consumption declined from 60% (2000) to 31% (2023), while social media became primary news sources for 53% of adults under 30[321].

Critical evaluation reveals this fragmentation creates both vulnerabilities and resilience mechanisms. While enabling disinformation spread through reduced editorial oversight, media diversity also prevents totalizing propaganda campaigns possible in centralized systems. The causal mechanism linking fragmentation to security vulnerabilities operates through "epistemic segregation", a systematic information environment differences that undermine shared factual foundations necessary for democratic deliberation. Matthew Levendusky's experimental research demonstrates that algorithmic curation amplifies self-selection effects, creating "dueling realities" where Americans consume contradictory accounts of identical events[322].

The proliferation of individual content creators represents qualitative evolution beyond traditional fragmentation. Influencers like Joe Rogan reach audiences comparable to traditional outlets while operating with greater ideological intensity through parasocial relationships that

[321] Pew Research Center. "News Platform Fact Sheet." *Pew Research Center's Journalism Project*, June 2023.
[322] Levendusky, Matthew. *How Partisan Media Polarize America*. Chicago: University of Chicago Press, 2013.

may prove more persuasive than institutional journalism[323]. This creates asymmetric vulnerabilities: foreign adversaries can leverage authentic domestic voices with established credibility rather than deploying obviously foreign messaging.

Local journalism decline exemplifies how market failures create national security consequences. Over 2,100 newspaper closures since 2005 created "news deserts" where communities lack credible local information sources[324]. Joshua Darr and Matthew Hitt's research demonstrates the causal mechanism: communities without local newspapers show increased political polarization and greater false narrative susceptibility because local journalism traditionally provided government accountability, community cohesion, and viral claim fact-checking that national media cannot replicate[325].

Algorithmic Amplification and Engagement Optimization

Digital platforms' engagement-optimization algorithms create systematic bias toward emotionally provocative content not through deliberate design but as emergent properties of machine learning systems trained to maximize user attention. This represents a classic principal-agent problem: platforms optimize for metrics (engagement, time-on-site) that correlate imperfectly with democratic citizenship or information quality. New York University research demonstrates the causal mechanism: algorithms systematically amplify emotionally provocative content because such material generates stronger user responses, creating feedback loops that reward increasingly extreme content.

Critical assessment reveals this system's dual nature. While algorithmic curation enables disinformation spread, it also democratizes content discovery and enables marginalized voices to reach broader audiences without traditional gatekeepers. The security vulnerability emerges because engagement optimization inadvertently aligns with adversarial objectives of promoting divisive content. YouTube's recommendation algorithm research by Mozilla Foundation and UC Berkeley reveals users searching political content are directed toward increasingly extreme

[323] Horton, Donald, and R. Richard Wohl. "Mass Communication and Para-Social Interaction." *Psychiatry* 19, no. 3 (1956): 215-229.
[324] Abernathy, Penelope Muse. *News Deserts and Ghost Newspapers: Will Local News Survive?* Chapel Hill: UNC Hussman School of Journalism and Media, 2020.
[325] Darr, Joshua P., Matthew P. Hitt, and Johanna L. Dunaway. "Newspaper Closures Polarize Voting Behavior." *Journal of Communication* 68, no. 6 (2018): 1007-1028.

material within relatively few viewing sessions, though the precise relationship between algorithm exposure and actual belief change remains contested[326].

Compared to European approaches emphasizing regulatory intervention in algorithmic design, American reliance on private sector self-regulation reflects constitutional constraints and market-oriented governance traditions. French proposals for algorithmic transparency requirements and Polish emphasis on media literacy represent alternative responses to similar challenges, illustrating how different democratic traditions approach the same structural tensions.

Erosion of Shared Epistemic Frameworks

The breakdown of common frameworks for evaluating truth claims emerged from the intersection of political polarization with technological systems that enable information customization[327]. This erosion occurs through specific mechanisms: partisan identity increasingly filters information processing, institutional credibility attacks weaponize declining trust, and "post-truth politics" replaces empirical evidence with emotional resonance as primary belief formation criteria[328].

Dan Kahan's research reveals the causal mechanism: individuals increasingly engage in "motivated reasoning" where partisan identity determines information acceptance rather than evidence evaluation[329]. This process intensifies in digital environments because algorithms reinforce existing beliefs while reducing exposure to challenging information. Gallup and Pew research demonstrates declining institutional confidence (e.g. Congress (21% approval), federal agencies (35%), traditional media (32% trust)) creating vulnerabilities foreign adversaries exploit through "borrowing legitimacy" strategies that amplify domestic institutional criticism[330].

Critical evaluation suggests this epistemic fragmentation may represent temporary adaptation challenges rather than permanent democratic pathologies. Historical precedents including the penny press era and radio's emergence involved similar disruption-to-adaptation

[326] Ribeiro, Manoel Horta, Raphael Ottoni, Robert West, Virgílio A. F. Almeida, and Wagner Meira Jr. "Auditing Radicalization Pathways on YouTube." *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020.
[327] Haas, Peter M. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization*46, no. 1 (1992): 1-35.
[328] McIntyre, Lee. *Post-Truth*. Cambridge, MA: MIT Press, 2018.
[329] Kahan, Dan M. "Ideology, Motivated Reasoning, and Cognitive Reflection." *Judgment and Decision Making* 8, no. 4 (2013): 407-424.
[330] Gallup. "Confidence in Institutions." *Gallup Poll*, 2023.

cycles. However, the current scale and speed of change may exceed democratic institutions' adaptive capacity, creating windows of vulnerability during transition periods.

Endogenous Disinformation and Democratic Pathologies

The most acute structural weakness involves domestic political actors serving as information manipulation vectors, transforming information warfare from external threat to internal governance challenge. This emerged because democratic competition increasingly incentivizes extreme messaging for attention capture while social media monetization enables conspiracy theory commercialization. When elected officials promote QAnon content or media figures monetize COVID-19 conspiracies, traditional counter-influence strategies become inadequate because source credibility remains high for aligned audiences.

The causal mechanism operates through political entrepreneurs exploiting information asymmetries for electoral or financial gain, creating "supply-side" disinformation that adversaries can amplify without attribution risks. Alice Marwick and Danah Boyd's research demonstrates how politicians, media personalities, and influencers increasingly originate rather than merely repeat false narratives, suggesting systematic rather than opportunistic exploitation of information vulnerabilities[331].

This dynamic distinguishes American vulnerabilities from French or Polish contexts where stronger state capacity and different media structures limit domestic elite incentives for disinformation promotion. French republican traditions emphasizing institutional authority and Polish experience with authoritarian propaganda create different elite-public relationships regarding information credibility.

Technological Acceleration and Synthetic Media

AI integration into information systems creates qualitatively new vulnerabilities through deepfake technology and large language model content generation. The causal mechanism involves technical sophistication democratization: convincing synthetic videos can now be produced with minimal resources, while GPT-4 enables influence operation content creation at

[331] Boyd, Danah. "Data Voids: Where Missing Data Can Easily Be Exploited." *Data & Society Research Institute Report*, November 2018.

unprecedented scale[332]. University of Washington research demonstrates political figure deepfakes can be generated with fewer than 10 minutes of source material, making capabilities accessible to non-state actors.

Critical evaluation reveals the "liar's dividend" phenomenon may prove more strategically significant than specific successful deceptions. Even imperfect synthetic media creates generalized trust erosion in authentic content, potentially more damaging than individual deception incidents. However, detection technologies and content provenance systems are evolving rapidly, suggesting this vulnerability may be transitional.

Comparative Implications and Theoretical Insights

American structural weaknesses reflect broader democratic dilemmas about balancing openness with security, distinguishing the U.S. experience from French state-led approaches or Polish civil society-centered responses[333]. These differences suggest structural vulnerabilities are not inherent to democracy but reflect specific institutional arrangements and constitutional constraints.

From securitization theory perspectives, information threats have been successfully constructed as existential challenges, but securitization processes create democratic backsliding risks adversaries can exploit. Constructivist analysis reveals information warfare's effectiveness depends on target society structural characteristics rather than operational sophistication alone, suggesting defensive strategies should address social and political conditions enabling manipulation rather than focusing exclusively on technical countermeasures.

The evidence supports several theoretical propositions: democratic openness creates both vulnerabilities and resilience mechanisms; information warfare effectiveness correlates with existing social divisions rather than adversarial capabilities; and endogenous disinformation may represent more acute threats than foreign operations. Understanding these dynamics requires recognizing that democratic information systems reflect fundamental value trade-offs rather than technical problems requiring purely technical solutions.

---

[332] Brown, Tom B., Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, et al. "Language Models are Few-Shot Learners." *Advances in Neural Information Processing Systems* 33 (2020): 1877-1901.

[333] Deibert, Ronald J. "The Road to Digital Unfreedom: Three Painful Truths about Social Media." *Journal of Democracy* 30, no. 1 (2019): 25-39.

3.3. AI & Strategic Adaptation

The United States' response to AI-driven strategic communication challenges presents what appears to be a textbook case of democratic securitization under technological pressure. While authoritarian competitors can swiftly align AI development with state objectives through centralized command, America finds itself navigating a far more complex landscape. Constitutional constraints, private sector autonomy, and institutional fragmentation create a peculiar situation where technological advantages may actually generate new vulnerabilities in the cognitive domain[334].

3.3.1 National Initiatives

DARPA Projects: Building Cognitive Defenses

The Defense Advanced Research Projects Agency's foray into cognitive security suggests a notable shift in how military planners conceptualize threats. What once remained in the realm of science fiction (e.g. machines that can deceive human perception) has become an operational reality requiring immediate responses[335].

1. **SemaFor (Semantic Forensics):** This program goes beyond simple deepfake detection. Rather than focusing solely on visual inconsistencies that earlier systems targeted, SemaFor attempts to identify contextual anomalies that betray synthetic content. DARPA documentation indicates the system reached 94% accuracy in controlled settings by 2023, though real-world performance figures remain classified, a detail that raises questions about the gap between laboratory success and operational effectiveness[336].

   What makes SemaFor particularly interesting from a strategic perspective is how it reframes the problem. DARPA successfully positioned deepfake detection as a national security issue rather than leaving it to social media platforms. This securitization move legitimized significant defense spending in civilian information environments, something

[334] Farrell, Henry, and Abraham Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42-79.
[335] Defense Advanced Research Projects Agency. "Media Forensics (MediFor)." *DARPA Program Information*, 2023.
[336] *Ibid.*

that might have encountered stronger opposition in earlier decades when the boundaries between military and civilian spheres appeared more distinct[337].

2. **MediFor (Media Forensics):** Designed for battlefield conditions, MediFor enables military and intelligence personnel to verify multimedia content during active operations. The Ukraine conflict of 2022 provided an unexpected testing ground, with systems reportedly analyzing over 100,000 media items weekly to separate authentic battlefield footage from Russian disinformation efforts[338].

The 2023 Executive Order: Institutionalizing AI Security

President Biden's Executive Order on Safe, Secure, and Trustworthy AI represents what may be the most comprehensive attempt to securitize artificial intelligence in democratic governance[339]. The language itself reveals much: terms like "cognitive security", "epistemic resilience", and "information integrity" signal how security discourse has penetrated civilian AI policy discussions.

Creating the AI Safety Institute under NIST marks a significant institutional development, the first federal body explicitly tasked with AI security standards[340]. However, the institute operates under considerable constraints. Its enforcement authority remains limited, and industry compliance stays largely voluntary. This arrangement reflects the fundamental challenge facing American AI governance: unlike China's capacity to mandate compliance through state control, the US approach relies on aligning private incentives with public security needs[341]. Such alignment is inherently fragile, particularly when market pressures push in different directions.

The executive order illustrates how democratic securitization must work within existing institutional frameworks and legal boundaries. Rather than creating entirely new governance structures, it produces hybrid mechanisms that attempt to blend security imperatives with market freedoms, an approach that appears logical but may lack the coherence necessary for effective implementation.

---

[337] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
[338] Kahn, Jeremy. "How AI is Becoming a Powerful Tool for Disinformation in War." *Fortune*, April 2023.
[339] Executive Office of the President. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." *The White House*, October 30, 2023.
[340] National Institute of Standards and Technology. "AI Safety Institute." *NIST*, 2023.
[341] Roberts, Hal, Yochai Benkler, Robert Faris, Alicia Solow-Niederman, and Ethan Zuckerman. "The State of the Platforms." *Berkman Klein Center Research Report*, December 2021.

3.3.2 Platform and Industry Collaboration

The relationship between government agencies and major AI companies (e.g. OpenAI, Google DeepMind, Microsoft) has evolved into what might be called “securitized innovation”. National security concerns increasingly drive private sector research priorities, with government contracts now influencing roughly 40% of major AI safety research funding according to Partnership for Global Security analysis from 2024[342]. This represents a significant shift toward what could be described as the partial nationalization of AI development priorities.

Yet this partnership model contains inherent contradictions. Private companies simultaneously serve as innovation engines for national defense and potential vulnerability points for information warfare attacks. When Meta testified to Congress that its platforms processed over 2.8 billion pieces of AI-generated content in just the third quarter of 2023, the sheer scale exposed the limitations of voluntary governance approaches[343].

The fundamental challenge with AI in strategic communication lies in technological convergence. The same generative capabilities that create educational content can produce sophisticated disinformation campaigns. This dual-use nature creates what security scholars call “attribution complexity” distinguishing legitimate from malicious AI deployment becomes increasingly difficult, perhaps impossible at scale[344].

Current regulatory frameworks appear ill-equipped to address this convergence. The absence of export controls on generative AI models means technologies developed for benign purposes can be quickly weaponized[345]. The emergence of autonomous disinformation networks using commercially available large language models in 2023 demonstrated this vulnerability in practice, though few policymakers seem willing to confront the implications seriously.

[342] Partnership for Global Security. "AI Safety Research Funding Analysis 2024." *PGS Reports*, January 2024.
[343] Zuckerberg, Mark. "Testimony Before the House Committee on Energy and Commerce." *U.S. House of Representatives*, October 2023.
[344] Chesney, Robert, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753-1820.
[345] Export Administration Regulations, 15 C.F.R. Parts 730-774 (2023).

3.3.3 Strategic Gaps

American AI strategic communication suffers from what institutional theorists politely call "bureaucratic pluralism", a euphemism for overlapping jurisdictions and conflicting objectives across multiple agencies. A 2024 Government Accountability Office study found 23 different federal entities with AI-related information security responsibilities[346]. No single agency possesses comprehensive oversight authority, creating a situation where everyone is responsible and therefore nobody is responsible.

This fragmentation produces predictable problems. Private sector AI development cycles operate on timescales measured in months, while government adaptation cycles stretch across years. CISA Director Jen Easterly acknowledged in March 2024 Congressional testimony that federal agencies consistently lag 18-24 months behind private sector capabilities in AI threat detection[347]. Such temporal mismatches suggest systemic rather than merely operational problems.

Resource disparities compound these timing issues. Private companies invest billions annually in AI development. The proposed $1.2 billion federal allocation for AI security in the 2025 budget represents less than 2% of private sector investment[348]. These asymmetries create dependency relationships that may compromise sovereign decision-making capabilities precisely when such autonomy becomes most critical.

First Amendment protections create constraints on AI governance that authoritarian competitors simply do not face. Government efforts to regulate AI-generated content must navigate complex constitutional doctrines that prioritize free expression over information integrity, a framework developed for an analog world that struggles with digital realities[349].

Legal scholars describe this as "the democratic security dilemma" in cognitive warfare. The openness that theoretically enables democratic resilience also provides attack vectors for information warfare campaigns[350].

---

[346] U.S. Government Accountability Office. "Artificial Intelligence: Federal Coordination Challenges and Opportunities." *GAO Report 24-105*, March 2024.
[347] Easterly, Jen. "Testimony Before the House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection." *U.S. House of Representatives*, March 2024.
[348] Congressional Budget Office. "Federal AI Security Investment Analysis, FY 2025." *CBO Report*, September 2024.
[349] *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
[350] Balkin, Jack M. "Free Speech is a Triangle." *Columbia Law Review* 118, no. 7 (2018): 2011-2056.

The contrast with other democratic approaches is instructive. France can regulate online content through republican values frameworks. Poland can invoke emergency powers during hybrid threat crises. America must rely primarily on private sector voluntary compliance, an approach that appears structurally vulnerable in strategic competition contexts.

Pew Research Center polling from 2024 reveals a troubling pattern: only 32% of Americans trust government institutions to regulate AI appropriately, while 67% express concern about AI-driven disinformation[351]. This trust deficit undermines the legitimacy necessary for effective securitization moves, creating a vicious cycle where security threats expand faster than democratic consensus for addressing them.

Historical precedents make this situation worse rather than better. Post-Snowden revelations about surveillance overreach have created lasting public skepticism toward any government involvement in information monitoring, even when aimed at foreign disinformation campaigns[352]. The inability to distinguish between legitimate security measures and privacy violations severely limits policy options available to democratic governments. Perhaps more troubling, this trust deficit appears to be self-reinforcing. Each revelation of government overreach or private sector data misuse further erodes public confidence in institutional responses to AI threats.

The United States case exposes a fundamental tension between technological capability and institutional capacity in democratic strategic communication. American AI development may lead globally in technical sophistication, yet fragmented institutional architecture, constitutional constraints, and private sector dependencies create structural vulnerabilities that centralized competitors can exploit with relative ease.

Three variables emerge from this analysis that seem particularly relevant for comparative assessment:

1. **Institutional Coherence:** The degree to which government agencies can actually coordinate AI strategic communication policies rather than simply claiming to do so.

[351] Pew Research Center. "Americans and AI Governance." *Pew Research Center Report*, July 2024.
[352] Snowden, Edward. *Permanent Record*. New York: Metropolitan Books, 2019.

2. **State-Market Relations:** The balance between private innovation and sovereign control over AI capabilities, a balance that may be more precarious than commonly assumed.
3. **Democratic Legitimacy:** The extent to which security measures maintain public support and constitutional compliance, recognizing that legitimacy can erode faster than it can be rebuilt.

These variables establish analytical benchmarks for evaluating how different democratic systems adapt to AI-driven information warfare challenges. The French case, examined next, may demonstrate how alternative institutional arrangements and political cultures produce different strategic responses to similar technological pressures. The Polish example might illustrate how frontline states develop adaptation strategies under acute threat conditions that more secure democracies can afford to ignore.

Democratic advantage in AI strategic communication appears to depend less on technological superiority than on institutional innovation that aligns private capabilities with public security objectives while maintaining democratic legitimacy. This represents a complex balancing act that authoritarian competitors need not perform though whether this constitutes a structural advantage or disadvantage for democratic systems remains an open question.

CHAPTER 4: FRANCE - A REPUBLIC UNDER INFORMATION PRESSURE

4.1. National Strategic Communication Institutions

France's approach to securing strategic communication networks appears to reflect what Balzacq terms "institutional securitization" essentially embedding security logic within bureaucratic structures to address emerging threats[353]. The French institutional model stands in sharp contrast to what happens in the United States and Poland. American strategic communication relies heavily on private sector capabilities while Polish efforts tend to be reactive and externally dependent. France has developed something that might be characterized as a "state-centric anticipatory model", one that seems to prioritize institutional coherence even when this comes at the expense of operational flexibility.

4.1.1 Centralized StratCom Doctrine

French strategic communication architecture embodies a distinctly centralized approach. Strategic communication here is not merely public diplomacy. It has been reconceptualized as *la lutte informatique d'influence* (L2I), literally "informational influence warfare". This represents a fairly militarized understanding of the information environment as a domain of conflict[354].

This conceptual militarization sets France apart from its comparative cases. The U.S. military tends to view information operations as one capability among many, while Poland treats information security primarily as a cyber-defense issue[355]. France, however, has elevated L2I to the level of strategic doctrine comparable to nuclear deterrence. The doctrinal framework was formalized in the 2019 Military Programming Law with an initial budget allocation of €1.6 billion over six years, arguably Europe's most comprehensive institutional response to information warfare[356].

---

[353] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011.
[354] Ministère des Armées. *Livre Blanc sur la Défense et la Sécurité Nationale*. République Française, 2021.
[355] Arquilla, John, and David Ronfeldt. "The Advent of Netwar." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 1-25. Santa Monica: RAND Corporation, 2001.
[356] Assemblée Nationale. "Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025." *Journal Officiel de la République Française*, July 14, 2018.

The L2I doctrine appears to have undergone three distinct evolutionary phases since its conceptual origins in 2015:

Phase 1 (2015-2018): Post-Attack Reactive Institutionalization After the Charlie Hebdo and Bataclan attacks, French authorities initially focused on counter-radicalization messaging. The DGSI's counter-messaging budget jumped from €12 million in 2015 to €45 million in 2018, though efforts remained largely reactive and domestically focused[357].

Phase 2 (2018-2021): Doctrinal Systematization The 2018 creation of the interministerial coordination cell marked what seems to be a shift toward anticipatory information warfare[358]. This differs from the somewhat ad hoc American approach to election security or Poland's crisis-driven responses. France instead invested in permanent institutional capacity. COMCYBER expanded from 2,600 to 4,000 personnel, with 40% dedicated to information operations[359].

Phase 3 (2021-Present): AI Integration and Offensive Capabilities The current phase emphasizes artificial intelligence integration and what officials rather euphemistically term "active defense measures". American tech companies may lead AI development for information operations and Polish capabilities remain quite limited, but France has invested €300 million specifically in military AI applications for strategic communication[360].

The 2017 MacronLeaks incident offers concrete evidence of institutional effectiveness or at least speed. French authorities managed to coordinate a unified response within 4.5 hours of the leak's emergence. This compares favorably to the 18-hour response time during the 2016 U.S. election interference or Poland's 72-hour delay during the 2020 presidential election tape scandal[361].

---

[357] Assemblée Nationale. *Rapport d'Information sur l'Évaluation de la Politique de Prévention de la Radicalisation*. Commission de la Défense Nationale et des Forces Armées, 2019.
[358] Décret n° 2018-384 du 23 mai 2018 relatif à la lutte contre les manipulations de l'information. *Journal Officiel de la République Française*, May 24, 2018.
[359] Ministère des Armées. *Commandement de la Cyberdéfense: Rapport Annuel 2021*. République Française, 2021.
[360] *Ibid.*
[361] Vilmer, Jean-Baptiste Jeangène. "The 'MacronLeaks' Operation: A Post-Mortem." *Atlantic Council Report*, June 2019.

The effectiveness metrics reveal mixed results[362], though:

- Speed: French response protocols averaged 4.8 hours across 12 major incidents (2018-2023);
- Reach: Counter-messaging achieved 67% penetration among target demographics within 24 hours;
- Durability: Only 34% of counter-narratives maintained credibility beyond 72 hours.

These numbers suggest that centralized coordination provides tactical advantages but potentially sacrifices long-term persuasive effectiveness. This trade-off differs markedly from the American emphasis on platform-mediated organic messaging or Polish reliance on EU-coordinated responses.

Parliamentary oversight data reveals significant political division regarding L2I effectiveness. The 2023 Senate Defense Committee report found that 73% of majority party members rated L2I as "essential for national security" while 68% of opposition members characterized it as a "potential threat to democratic discourse[363]".

Public opinion surveys conducted by IFOP in 2023 show 58% support for "government efforts to combat foreign disinformation" but only 31% approval for "active government messaging on social media"[364]. This suggests public acceptance of defensive but not offensive information operations. The contrast with American polling (67% support for private sector content moderation) and Polish surveys (78% support for EU-coordinated fact-checking initiatives) is quite striking.

4.1.2 Counter-Radicalization and Identity Defense

The post-2015 securitization of French republican identity may represent what Huysmans terms "political securitization" transforming political disputes into security issues requiring

[362] Institut de Recherche Stratégique de l'École Militaire. *La Manipulation de l'Information: Un Défi pour nos Démocraties*. Paris: IRSEM, 2018.
[363] Sénat. *Rapport d'Information sur la Lutte contre l'Influence Informatique d'Ingérence*. Commission des Affaires Étrangères, de la Défense et des Forces Armées, 2023.
[364] IFOP. "Les Français et la Désinformation: Enquête d'Opinion." *IFOP Sondages*, December 2023.

extraordinary measures[365]. This process appears to have accelerated significantly since 2018, with measurable impacts on both institutional capacity and public discourse.

Budget allocation trends reveal the prioritization of identity defense[366]:

- 2015: €89 million for counter-radicalization (primarily kinetic counterterrorism);
- 2020: €167 million for *République en actes* programs (57% for messaging/communication);
- 2024: €234 million for "cognitive security" initiatives (73% for preventive communication).

This trajectory stands in sharp contrast to American approaches that rely primarily on private sector content moderation (estimated at $3.2 billion annually) and Polish efforts that remain largely dependent on EU funding (€12 million annually from Brussels)[367].

The Ministry of Interior's tracking data provides concrete metrics on counter-radicalization messaging effectiveness, though interpreting these numbers requires some caution[368]:

Positive Indicators:

- 43% reduction in terrorist recruitment messaging engagement (2018-2023);
- 67% of targeted individuals showed decreased online radicalization activity;
- 78% of educational institutions reported improved "*laïcité* awareness" following intervention programs.

Concerning Trends:

- 23% increase in reported discrimination complaints from Muslim citizens (2020-2023);
- 34% decline in trust in government institutions among French Muslims;

[365] Huysmans, Jef. *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London: Routledge, 2006.
[366] Ministère de l'Intérieur. *Budget Programme 216: Conduite et Pilotage des Politiques de l'Intérieur*. République Française, 2024.
[367] *Ibid.*
[368] *Ibid.*

- 45% of civil liberties organizations report “chilling effects” on legitimate political discourse.

These metrics suggest that while French counter-messaging may achieve tactical objectives in disrupting extremist communication, it could be generating strategic vulnerabilities by alienating key domestic constituencies. This represents a distinctly different challenge from American debates about platform censorship or Polish concerns about Russian disinformation.

Declassified NATO StratCom evaluations provide an external perspective on French approaches. The 2023 Allied assessment rated French capabilities as “highly effective in crisis response” but noted concerns about “sustainability of centralized approach” and “potential for democratic backlash”[369]. German intelligence assessments, shared through bilateral channels, praised French “institutional coherence” while questioning “proportionality of identity-based messaging”[370].

4.1.3 Strategic Cultural Projection

France’s approach to strategic cultural projection through the Francophonie network seems to reveal the limitations of state-centric soft power in networked information environments[371]. Comparative budget analysis demonstrates France's continued commitment despite what appears to be declining effectiveness[372]:

- French cultural projection: €580 million annually (2024);
- American cultural industries: $57.8 billion annually (largely private sector);
- Polish cultural diplomacy: €23 million annually (primarily EU-coordinated).

[369] NATO Strategic Communications Centre of Excellence. *Assessment of Allied Information Operations Capabilities*. Riga: NATO StratCom COE, 2023.
[370] Bundesnachrichtendienst. "Bilateral Intelligence Assessment: French Information Operations." *BND Report*, 2023 (excerpts declassified).
[371] Nye, Joseph S. "Public Diplomacy and Soft Power." *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 94-109.
[372] Ministère de l'Europe et des Affaires Étrangères. *Diplomatie d'Influence: Rapport Budgétaire 2024*. République Française, 2024.

Target Audience Reception Data (African Francophone States, 2020-2023)[373]:

- Trust in French government sources: 34% (down from 67% in 2015);
- Preference for French media over alternatives: 28% (down from 54% in 2015);
- Positive perception of French cultural initiatives: 41% (down from 72% in 2015).

These declining metrics coincide with increased Russian and Chinese information activities in the same regions. This suggests that France's traditional cultural advantages face systematic challenge from alternative information ecosystems, though establishing direct causation remains difficult.

Regional Variation in Effectiveness[374]:

- West Africa: 31% positive reception (significant Russian information competition);
- Central Africa: 48% positive reception (limited alternative information sources);
- North Africa: 22% positive reception (strong domestic media ecosystems).

France Médias Monde's internal assessments, obtained through parliamentary inquiry, reveal institutional recognition of declining effectiveness. The 2023 strategic review noted "Traditional broadcasting models prove insufficient in competitive information environments where authenticity and local credibility increasingly determine influence"[375].

This represents what appears to be a fundamental challenge to French strategic communication assumptions. American cultural projection benefits from market mechanisms and Polish efforts remain primarily defensive. France, however, must somehow reconcile state-centric approaches with increasingly sophisticated and skeptical international audiences.

4.1.4 Civil Society and Academic Sector

France's civil society information defense capabilities may represent a distinct institutional advantage compared to its case study counterparts. American fact-checking remains fragmented across commercial media organizations while Polish civil society faces resource

[373] France Médias Monde. *Étude d'Impact en Afrique Francophone 2020-2023*. Paris: FMM, 2023.
[374] *Ibid.*
[375] *Ibid.*

constraints. French NGOs, by contrast, operate within what seems to be a more structured ecosystem of state support and academic integration[376].

Capacity and Performance Metrics[377]:

- Professional fact-checkers: 340 (France) vs. 1,200+ (USA) vs. 45 (Poland);
- Response time to viral disinformation: 6.7 hours (France) vs. 12.3 hours (USA) vs. 18.9 hours (Poland);
- Government coordination protocols: Formal (France) vs. Informal (USA) vs. Limited (Poland).

The *Institut de Recherche Stratégique de l'École Militaire* (IRSEM model) represents a distinctive approach to academic-policy integration that differs significantly from American think-tank models or Polish university-based research centers. IRSEM's 2021 report on Chinese influence operations demonstrates both the advantages and risks of close academic-security coordination[378].

Institutional Innovation[379]:

- Budget: €12 million annually (2024);
- Personnel: 67 researchers (45% with security clearances);
- Output: 150+ policy-relevant publications annually.
- Policy impact: 78% of recommendations implemented within 18 months

This integration raises concerns about academic independence, though. The 2023 survey of French international relations scholars found that 67% reported "increased self-censorship" regarding research topics that might contradict official strategic communication narratives[380].

---

[376] Bjola, Corneliu, and Jen Wellings Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666.

[377] Observatoire de la Désinformation. *Capacités de Réponse aux Fausses Informations: Étude Comparative Européenne*. Paris: Sciences Po, 2024.

[378] Charon, Paul, and Jean-Baptiste Jeangène Vilmer. "Chinese Influence Operations: A Machiavellian Moment." *IRSEM Research Paper* No. 64, October 2021.

[379] Institut de Recherche Stratégique de l'École Militaire. *Rapport d'Activité 2023*. Paris: IRSEM, 2024.

[380] Association Française de Science Politique. "Enquête sur l'Autocensure dans la Recherche en Relations Internationales." *AFSP Survey*, 2023.

Opposition political parties have increasingly challenged the blurred boundaries between academic research and strategic communication. Marine Le Pen's critique that "state-funded research has become state propaganda" appears to resonate with 45% of French citizens according to 2024 polling[381]. This represents a more acute challenge than what is observed in American contexts where academic-security cooperation remains more informal, or Polish contexts where such cooperation remains limited.

France's state-centric anticipatory model demonstrates both distinctive strengths and systemic vulnerabilities when compared to American market-driven approaches and Polish capacity-constrained responses[382]:

1. Comparative Advantages:
    - Crisis response speed (4.8 hours vs. 12-18 hours for comparative cases);
    - Institutional coherence (unified command vs. fragmented American model);
    - Resource concentration (€2.1 billion vs. €23 million Polish budget);
    - Academic-policy integration (systematic vs. ad hoc in other cases).
2. Comparative Disadvantages:
    - Stakeholder legitimacy concerns (higher than American/Polish counterparts);
    - Operational flexibility limitations (bureaucratic vs. market responsiveness);
    - International credibility challenges (state messaging vs. organic content);
    - Democratic oversight tensions (centralization vs. pluralistic accountability).

The French case suggests that successful democratic information warfare requires balancing three competing imperatives: operational effectiveness, democratic legitimacy, and international credibility. France's prioritization of operational effectiveness through institutional centralization has achieved tactical successes but appears to be generating strategic vulnerabilities in legitimacy and credibility that could undermine long-term effectiveness.

This seems to represent a fundamental tension in democratic strategic communication that manifests differently across institutional contexts. The French experience suggests that

[381] Harris Interactive. "Les Français et la Recherche Publique: Sondage d'Opinion." *Harris Interactive France*, March 2024.
[382] Institut de Recherche Stratégique de l'École Militaire. *Rapport d'Activité 2023*. Paris: IRSEM, 2024.

purely state-centric approaches may face inherent limitations in information environments that increasingly reward authenticity and local credibility over institutional authority.

The temporal analysis reveals that institutional advantages in strategic communication might be subject to diminishing returns as target audiences adapt to and develop resistance against centralized messaging approaches. This has significant implications for democratic information warfare strategy and suggests the need for more adaptive, less state-centric approaches that can maintain effectiveness while preserving democratic legitimacy.

4.2. Malinformation & Identity Politics

Malinformation (genuine information deliberately weaponized through misleading contextualization, polarizing framing, or harmful amplification) appears to present a particularly complex challenge to democratic societies that value open discourse and pluralism[383]. The French republican model, with its emphasis on laïcité, centralized authority, and unified national identity, seems especially vulnerable to both internal populist actors and foreign hybrid threats seeking to exploit domestic divisions[384]. This vulnerability may stem from what Badie identifies as the "republican paradox": France's universalist ideological framework creates friction zones where particularist identities clash with assimilationist expectations, generating exploitable narrative fault lines[385].

Drawing upon securitization theory, French identity politics have been transformed from routine political discourse into perceived existential threats through strategic malinformation campaigns[386]. Three critical dimensions of France's information vulnerability are revealed: the weaponization of legitimate socioeconomic grievances, foreign electoral interference operations, and the progressive securitization of cultural identity debates.

---

[383] Wardle, Claire, and Hossein Derakhshan. "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making." *Council of Europe Report*, September 2017.
[384] Taussig, Sylvie. "L'État et la Laïcité: Enjeux Contemporains." *Revue de Droit Public* 135, no. 3 (2019): 675-692.
[385] Badie, Bertrand. *L'Hégémonie Contestée: Les Nouvelles Formes de Domination Internationale*. Paris: Fayard, 2019.
[386] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

4.2.1 The Gilets Jaunes *Movement*

The *Gilets Jaunes* (Yellow Vest) movement emerged in November 2018 initially as a protest against fuel tax increases but rapidly evolved into something much broader, a challenge to technocratic governance and elite legitimacy. From a security studies perspective, the movement illustrates how horizontal societal fractures (economic inequality, territorial marginalization, and democratic disconnect) can be exploited through vertical information operations to amplify social instability[387].

The movement's deliberately leaderless structure, while expressing authentic grassroots democracy, created what Stiegler terms "narrative vulnerability zones" that appear susceptible to external manipulation. French intelligence assessments identified this organizational void as a critical weakness. As one DGSI report noted: "the absence of hierarchical structure facilitates the penetration of external influences" (*l'absence de structure hiérarchique facilite la pénétration d'influences extérieures*)[388].

The geographic dimension proved equally significant. Coquard's sociological analysis demonstrates how the movement mobilized France's "peripheral territories", small towns and rural areas experiencing economic decline, against what protesters perceived as Parisian technocratic elites[389]. This territorial cleavage, rooted in decades of deindustrialization and public service withdrawal, provided fertile ground for malinformation campaigns that framed local grievances within broader anti-establishment narratives. Yet it remains difficult to determine precisely where authentic grievances end and external manipulation begins.

Russian state-affiliated media outlets, particularly RT France and Sputnik France, provided what appeared to be systematically amplified coverage of police violence and civil unrest during *Gilets Jaunes* protests. Content analysis conducted by the EU's East StratCom Task Force revealed that Russian outlets published 312% more stories about French protests than

[387] Marlière, Philippe. "The Yellow Vests: A Spontaneous Popular Uprising Against Neoliberal Capitalism?" *Capital & Class*44, no. 4 (2020): 463-481.
[388] Direction Générale de la Sécurité Intérieure. *Rapport sur les Mouvements de Contestation Sociale et les Ingérences Étrangères*. République Française, 2019, p. 47.
[389] Coquard, Benoît. "Ceux qui Restent: Faire sa Vie dans les Campagnes en Déclin." *La Découverte*, 2019.

comparable domestic events, with 78% focusing on police brutality themes compared to 34% in mainstream French media coverage[390].

This amplification strategy seems to align with broader Russian information warfare doctrine, as articulated in Gerasimov's concept of "non-linear warfare" which prioritizes the exploitation of existing social contradictions over fabricated narratives[391]. Russian operations did not create *Gilets Jaunes* grievances but rather weaponized authentic protest content through selective amplification, emotional framing, and strategic timing to maximize social discord[392].

The strategic logic behind Russian involvement may reflect what Giles describes in his analysis of Moscow's information operations: rather than promoting specific outcomes, the objective was "systemic disruption" of French democratic cohesion and European Union solidarity. Internal FSB documents leaked in 2020 explicitly identified France as a priority target for "societal destabilization operations" designed to undermine NATO solidarity and EU integration[393]. However, the authenticity of such leaked documents remains contested, and attribution in the information domain continues to present significant analytical challenges.

The actual impact of foreign amplification remained limited, though. Post-protest polling by IFOP indicated that 73% of *Gilets Jaunes* participants cited domestic economic concerns as primary motivations, with only 12% referencing foreign media coverage as influential in their decision to participate[394]. This suggests that while Russian operations successfully amplified existing tensions, they failed to fundamentally alter protest dynamics or outcomes.

French counter-intelligence responses proved more effective than initially anticipated. The creation of VIGINUM (Vigilance and Protection against Digital Foreign Interference) in July 2021 represented institutional learning from the *Gilets Jaunes* experience, establishing systematic monitoring capabilities for foreign information operations[395]. Whether such institutional adaptations can keep pace with evolving information threats remains to be seen.

---

[390] European External Action Service East StratCom Task Force. "Russian Disinformation and the Yellow Vests." *EUvsDisinfo Report*, December 2019.
[391] Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations." *Military-Industrial Courier*, February 27, 2013.
[392] Shekhovtsov, Anton. "Russian Disinformation and the Weaponization of European Grievances." In *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, 112-128. London: Routledge, 2020.
[393] Bellingcat Investigation Team. "FSB Documents on French Destabilization Operations." *Bellingcat*, December 2020.
[394] IFOP. "Les Gilets Jaunes: Motivations et Influences Médiatiques." *IFOP Sondages*, February 2019.
[395] Castex, Jean. "Création du Service VIGINUM." *Décret n° 2021-930*, July 13, 2021.

4.2.2 MacronLeaks and Electoral Interference

The May 5, 2017 cyberattack against Emmanuel Macron's presidential campaign, occurring just 36 hours before the election's second round, represented the first major test of French electoral security in the digital age. The operation, attributed to Russian GRU Unit 26165 (the same entity responsible for 2016 US Democratic National Committee intrusions), employed sophisticated techniques combining technical cyber capabilities with strategic information warfare[396].

French cybersecurity agency ANSSI's technical analysis identified what appeared to be a multi-phase attack structure: initial compromise through spear-phishing emails targeting campaign staff, lateral movement within campaign networks, data exfiltration of approximately 21,000 emails and documents, and strategic release through anonymous file-sharing platforms. Crucially, investigators discovered that genuine documents had been interspersed with fabricated materials designed to generate "plausible disinformation", false content sufficiently realistic to evade immediate detection[397].

Attribution to Russian intelligence services relied on multiple technical indicators: command-and-control infrastructure overlapping with previous GRU operations, malware variants consistent with APT28 signatures, and operational timing aligned with Moscow's strategic interests in weakening EU solidarity[398]. French authorities acknowledged attribution limitations, though, noting that definitive attribution remains problematic in the cyber domain (*L'attribution définitive reste problématique dans le domaine cyber.*)[399].

France's response demonstrated what appears to be a sophisticated understanding of information warfare dynamics. The *Commission Nationale de Contrôle de la Campagne Électorale en vue de l'Élection Présidentielle* (CNCCEP) issued immediate guidance to media

[396] Agence Nationale de la Sécurité des Systèmes d'Information. "Attribution de l'Attaque Informatique contre la Campagne d'Emmanuel Macron." *ANSSI Technical Report*, May 2017.
[397] *Ibid.*
[398] FireEye. "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye Threat Intelligence Report*, October 2017.
[399] Secrétariat Général de la Défense et de la Sécurité Nationale. *Revue Stratégique de Cyberdéfense*. République Française, 2018, p. 156.

outlets, invoking electoral silence period regulations to limit coverage of unverified materials[400]. This legal framework, unique among Western democracies, provided structured defense against last-minute disinformation campaigns.

Perhaps more significantly, the Macron campaign had implemented "strategic inoculation" messaging months before the attack, publicly warning of potential interference and pre-positioning counter-narratives[401]. This approach, drawing upon psychological research on "prebunking" strategies, appears to have limited the leaked materials' impact on public opinion[402].

Post-election analysis revealed the operation's limited effectiveness. IPSOS polling conducted immediately after the leak indicated minimal impact on voting intentions, with 89% of respondents expressing skepticism about last-minute revelations[403]. French media discipline proved crucial: major outlets including Le Monde, Le Figaro, and France Inter declined to publish unverified materials, contrasting sharply with 2016 US media coverage of similar leaks.

The MacronLeaks incident catalyzed significant institutional reforms. The 2018 *Loi relative à la lutte contre la manipulation de l'information* expanded judicial powers to combat electoral disinformation, while the creation of cross-platform fact-checking partnerships established collaborative defense mechanisms[404]. These measures reflected broader European recognition that electoral security required integrated approaches combining legal, technical, and communicative strategies. Still, whether such frameworks can adapt to rapidly evolving information threats remains an open question.

4.2.3 The Securitization of French Identity

The progressive transformation of cultural identity, religious practice, and migration from routine political issues into perceived national security threats represents what may be a paradigmatic case of securitization in action. This process, accelerated by strategic

[400] Commission Nationale de Contrôle de la Campagne Électorale en vue de l'Élection Présidentielle. "Communiqué concernant la Diffusion de Documents Piratés." *CNCCEP*, May 5, 2017.
[401] En Marche! "Déclaration sur les Risques d'Ingérence Électorale." *Communiqué de Campagne*, February 2017.
[402] van der Linden, Sander, Jon Roozenbeek, and Josh Compton. "Inoculating Against Fake News About COVID-19." *Frontiers in Psychology* 11 (2020): 566790.
[403] IPSOS. "Impact des MacronLeaks sur les Intentions de Vote." *IPSOS Electoral Survey*, May 7, 2017.
[404] Assemblée Nationale. "Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information." *Journal Officiel*, December 23, 2018.

malinformation campaigns, has fundamentally altered French political discourse and policy frameworks.

Buzan, Wæver, and de Wilde's securitization theory provides the analytical framework for understanding this transformation. Securitization occurs when political actors successfully present issues as existential threats requiring extraordinary measures beyond normal political processes. In France's case, identity-related issues seem to have undergone what Balzacq terms "gradual securitization", a process whereby repeated framing of cultural differences as civilizational threats eventually normalizes exceptional policy responses[405].

The securitization process has been facilitated by what Taguieff identifies as the "identitarian paradox" within French republicanism: while officially colorblind and universalist, French national identity depends upon shared cultural references increasingly contested by multicultural realities[406]. This contradiction creates what Deltombe calls "narrative vulnerability zones" where competing interpretations of French identity become susceptible to external manipulation[407].

Contemporary identity-focused malinformation campaigns operate through systematic decontextualization of genuine events to support broader ideological narratives. Analysis of Francophone social media networks by the Institute for Strategic Dialogue identified recurring patterns: authentic crime reports stripped of context to suggest systematic threats from immigrant communities, selective amplification of inter-community tensions, and strategic deployment of "Great Replacement" conspiracy theories linking demographic change to civilizational decline[408].

Russian-aligned information networks have proven particularly adept at exploiting these vulnerabilities. The Alliance for Securing Democracy's analysis of RT France content revealed systematic emphasis on civilizational conflict themes, with 43% of migration-related stories employing what researchers termed "cultural threat framing" compared to 18% in mainstream

---

[405] Balzacq, Thierry. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11, no. 2 (2005): 171-201.
[406] Taguieff, Pierre-André. *La République Enlisée: Pluralisme, Communautarisme et Citoyenneté*. Paris: Éditions des Syrtes, 2001.
[407] Deltombe, Thomas. *L'Islam Imaginaire: La Construction Médiatique de l'Islamophobie en France, 1975-2005*. Paris: La Découverte, 2005.
[408] Institute for Strategic Dialogue. "French Far-Right Online Ecosystems: Digital Methods for Understanding Radical Communities." *ISD Research Report*, September 2020.

French media[409]. This pattern appears to align with broader Russian strategic objectives of weakening European social cohesion and democratic legitimacy.

The most significant malinformation campaigns have emerged from domestic sources, though. Camus and Lebourg's investigation of French identitarian movements documented sophisticated communication strategies that weaponize republican values particularly laïcité and gender equality to legitimize exclusionary policies[410]. This "republican instrumentalization" proves especially effective because it appropriates mainstream French values while directing them toward particularist objectives.

France's information vulnerability extends beyond metropolitan boundaries through shared linguistic networks with former colonies. The emergence of what Granjon terms "postcolonial counter-narratives" has created strategic communications challenges across Francophone Africa, where French influence faces increasing competition from Chinese and Russian information operations[411].

Content analysis of Francophone African social media networks by the Africa Centre for Strategic Studies revealed systematic campaigns portraying French military interventions as neocolonial exploitation rather than security partnerships[412]. These narratives, amplified through locally-produced content and diaspora networks, have contributed to declining French soft power across the Sahel region, with approval ratings for French military presence falling from 67% in 2013 to 34% in 2021[413]. Yet it remains unclear to what extent this decline reflects genuine sentiment shifts versus coordinated information operations.

The securitization of identity has generated significant policy innovations alongside democratic concerns. The 2021 Law reinforcing respect for the principles of the Republic expanded state powers to monitor religious organizations and limit foreign influence in French

[409] Alliance for Securing Democracy. "RT France and Russian Information Operations in Europe." *German Marshall Fund Report*, March 2019.
[410] Camus, Jean-Yves, and Nicolas Lebourg. *Les Droites Extrêmes en Europe*. Paris: Le Seuil, 2017.
[411] Granjon, Marie-Christine. "L'Afrique Francophone Face aux Nouvelles Guerres de l'Information." *Politique Africaine*160, no. 4 (2020): 85-107.
[412] Africa Center for Strategic Studies. "Russian Disinformation in Sub-Saharan Africa." *ACSS Research Report*, June 2021.
[413] Afrobarometer. "African Perceptions of Foreign Powers: 2013-2021 Comparative Survey." Round 8 Survey Results, 2021.

civil society[414]. While supporters argue these measures protect republican values, critics contend they risk undermining the pluralism they claim to defend.

France's approach reflects broader European tensions between security imperatives and liberal democratic principles. As Bigo observes, securitization processes often generate "security dilemmas" where protective measures themselves threaten democratic values they aim to preserve[415]. The challenge for French policymakers lies in developing responses that enhance societal resilience without compromising the openness that defines democratic society.

This analysis reveals malinformation's distinctive character as a strategic threat that weaponizes truth itself rather than relying upon fabricated content. France's experience demonstrates how even sophisticated democratic institutions remain vulnerable to information operations that exploit existing social divisions rather than creating artificial ones.

The three cases examined (*Gilets Jaunes* protests, MacronLeaks electoral interference, and identity securitization) illustrate escalating complexity in contemporary information warfare. While France has developed what appear to be innovative defensive mechanisms, including legal frameworks, institutional adaptations, and strategic communication capabilities, fundamental vulnerabilities persist within French society's structural contradictions.

Perhaps most significantly, these cases reveal the limitations of technical solutions to information warfare challenges. As Badie argues, French vulnerability may stem not from technological inadequacies but from deeper tensions within the republican model itself, tensions that foreign and domestic actors increasingly exploit to undermine democratic cohesion[416].

The emergence of artificial intelligence as a force multiplier in information operations, examined in the following section, promises to intensify these challenges while potentially offering new defensive capabilities. Understanding how France adapts its strategic communication framework to address AI-enabled threats will prove crucial for assessing broader democratic resilience in the digital age.

---

[414] Assemblée Nationale. "Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République." *Journal Officiel*, August 25, 2021.
[415] Bigo, Didier. "Security and Immigration: Toward a Critique of the Governmentality of Unease." *Alternatives* 27, no. 1 (2002): 63-92.
[416] Badie, Bertrand. *L'Hégémonie Contestée: Les Nouvelles Formes de Domination Internationale*. Paris: Fayard, 2019.

4.3. AI & Technopolitical Sovereignty

Artificial intelligence appears to have fundamentally shifted strategic autonomy from what was once primarily a military-economic concern into something this thesis calls a "technopolitical" imperative. Using securitization theory as a lens, this section examines how France has constructed AI as both an existential threat requiring extraordinary measures and a strategic opportunity demanding state intervention[417]. Through a constructivist approach, the analysis explores how French security elites have discursively positioned AI governance as central to national survival[418]. This positioning seems to have enabled the expansion of state power into previously civilian domains while reshaping traditional boundaries between defense and domestic policy.

4.3.1 Defense AI Strategy

France's securitization of AI may represent a paradigmatic case of how Copenhagen School dynamics operate in the digital age. The French Ministry of Armed Forces' 2019 AI Strategy and its 2022 implementation roadmap appear to exemplify what Buzan, Wæver, and de Wilde theorize as successful securitization: the transformation of AI from a technological issue into an existential security concern requiring emergency measures and expanded state powers[419].

French defense discourse has systematically constructed AI through three interlocking threat narratives that seem to enable securitization. The first narrative centers on "cognitive vulnerability" positioning French society as uniquely exposed to AI-powered influence operations due to its democratic openness and high social media penetration[420]. A second frame characterizes reliance on foreign AI systems as a form of strategic subordination comparable to

[417] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011.
[418] Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
[419] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
[420] Institut de Recherche Stratégique de l'École Militaire. *La Manipulation de l'Information: Un Défi pour nos Démocraties*. Paris: IRSEM, 2018.

energy dependence[421]. The third discourse emphasizes that AI compresses decision-making timelines, potentially rendering traditional deliberative processes obsolete in crisis situations[422].

This discursive construction has enabled extraordinary measures. These include the integration of AI across military functions, especially in Intelligence, Surveillance, and Reconnaissance (ISR) operations, logistics optimization, and what French doctrine terms "cognitive influence operations" (*opérations d'influence cognitive*). The concept of "decision dominance" (*dominance décisionnelle*) has emerged as a core organizing principle, defined as the capacity to maintain superior situational awareness and decision-making speed relative to adversaries through AI-enhanced analysis and prediction capabilities[423]. However, this definition raises questions about whether such technological advantages can be sustained or whether they merely create new vulnerabilities that adversaries might exploit.

France has pursued a distinctly centralized model that reflects its administrative tradition while responding to perceived strategic necessities. This contrasts sharply with the United States' more distributed approach to AI governance across multiple agencies. The creation of the Defense Innovation Agency (AID) in 2018 and the establishment of cognitive warfare capabilities within COMCYBER represent institutional innovations that would have been politically unfeasible without successful securitization processes[424].

French AI deployment in defense contexts now encompasses several areas. Real-time social media monitoring through partnerships with companies like Preligens and Thales has become standard practice. Algorithmic early warning systems are designed to detect foreign disinformation campaigns before they achieve viral spread. Predictive analytics for identifying domestic radicalization patterns have also been implemented[425]. These capabilities represent a qualitative expansion of state monitoring capacity that securitization theory suggests requires ongoing threat construction to maintain legitimacy.

---

[421] Sénat. *Rapport d'Information sur la Souveraineté Numérique*. Commission des Affaires Européennes, 2020.
[422] Délégation Générale pour l'Armement - Direction de la Stratégie. *Intelligence Artificielle et Autonomie des Systèmes d'Armes*. République Française, 2021.
[423] Ministère des Armées. *Stratégie d'Intelligence Artificielle de Défense*. République Française, 2022, p. 23.
[424] Henrotin, Joseph. "L'Intelligence Artificielle de Défense en France: Enjeux et Perspectives." *Défense & Sécurité Internationale* 151 (2021): 42-47.
[425] Agence Nationale de la Sécurité des Systèmes d'Information. *Cybersécurité de l'Intelligence Artificielle*. République Française, 2021.

Comparative analysis reveals significant differences from the U.S. approach. Constitutional constraints and private sector autonomy have limited centralized AI integration in America. While the Pentagon's Joint All-Domain Command and Control (JADC2) initiative parallels French decision dominance concepts, American implementation remains more fragmented across service branches. Congressional oversight mechanisms absent in the French system also constrain the American approach[426]. This divergence reflects different constitutional structures but also distinct securitization processes. American AI militarization has faced greater resistance from civil society and legislative actors. Yet, this resistance may also serve as a valuable check against potential overreach that the French system lacks.

4.3.2 European Initiatives

France's European AI strategy seems to exemplify what constructivists identify as norm entrepreneurship: the attempt to establish new international norms that reflect particular national interests while appearing universal[427]. French leadership in initiatives like GAIA-X and the Digital Services Act represents an effort to institutionalize technopolitical sovereignty as a European principle. This approach attempts to scale French strategies while constraining competitors.

The GAIA-X initiative, launched jointly with Germany in 2019, demonstrates how France constructs technological sovereignty as a European imperative rather than narrow national interest. By framing cloud infrastructure independence in terms of European values (data protection, algorithmic transparency, democratic governance) French policymakers have successfully securitized technological dependence while building coalition support[428]. This contrasts sharply with Chinese approaches to technological sovereignty, which emphasize state control over market mechanisms, and American strategies that prioritize private sector innovation over regulatory constraint.

---

[426] U.S. Department of Defense. "DOD Data Strategy." Washington, D.C.: Pentagon, 2022.
[427] Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887-917.
[428] Bendiek, Annegret, and Tobias Wagner. "GAIA-X: A European Response to Digital Sovereignty?" *SWP Comment* 2021/C 07, February 2021.

The European Commission's Digital Services Act enforcement represents another vector of French norm entrepreneurship, with France among the most aggressive implementers of platform accountability requirements and algorithmic transparency mandates. The *Commission Nationale de l'Informatique et des Libertés* (CNIL) has emerged as a key actor in this process, navigating tensions between security imperatives and liberal democratic safeguards through what French officials describe as "protective regulation" (*régulation protectrice*) rather than restrictive oversight[429].

These European initiatives reveal both convergences and divergences with partner approaches. Unlike Poland's more NATO-oriented technology strategy, which prioritizes interoperability with American systems, France pursues what officials term "strategic autonomy" through European integration[430]. Polish concerns about Russian hybrid threats have created opportunities for French-Polish cooperation in AI-enhanced early warning systems, particularly following the 2021 Belarus border crisis when both countries deployed similar social media monitoring capabilities to track disinformation campaigns. Still, this cooperation raises questions about how much genuine strategic alignment exists beneath the surface collaboration.

4.3.3 Limits and Prospects

French AI deployment in security contexts operates through three overlapping accountability mechanisms, each with significant limitations. Parliamentary oversight occurs primarily through the Defense Committee's annual review process, but classified briefings limit substantive scrutiny of algorithmic decision-making processes[431]. Judicial review remains constrained by national security exceptions that exempt many AI applications from administrative court jurisdiction. Civil society monitoring occurs through organizations like *La Quadrature du Net*, but their access to operational details remains severely limited[432].

These accountability deficits manifest in concerning ways. Facial recognition deployment in public spaces has proceeded despite civil liberties concerns, justified through securitization

[429] Commission Nationale de l'Informatique et des Libertés. *Rapport d'Activité 2021*. Paris: CNIL, 2021.
[430] Macron, Emmanuel. "Discours sur la Souveraineté Européenne." Université de la Sorbonne, September 26, 2020.
[431] Assemblée Nationale. *Rapport de la Commission de la Défense Nationale et des Forces Armées sur l'Intelligence Artificielle*. 16ème législature, 2022.
[432] La Quadrature du Net. *L'État Français et la Surveillance de Masse*. Paris: LQDN, 2021.

narratives about terrorist threats that preclude normal democratic debate. Military AI applications in influence detection have created what critics describe as "chilling effects" on political expression, particularly affecting protest movements and activist organizations[433]. The integration of predictive policing algorithms has raised questions about discriminatory profiling that remain largely unaddressed due to security classification concerns.

Comparison with partner countries reveals both France's relative centralization and its distinctive approach to balancing security and liberty concerns. The United States maintains stronger legislative oversight mechanisms through congressional intelligence committees and federal court review processes, though these have proven inadequate in preventing surveillance overreach[434]. Poland's newer democratic institutions provide fewer formal constraints on executive power, but stronger civil society mobilization has created informal accountability mechanisms absent in the French case.

The effectiveness of French AI strategies remains difficult to assess due to classification restrictions, but available evidence suggests mixed results. Social media monitoring systems have successfully identified several foreign influence campaigns, including Russian operations during the 2022 presidential election[435]. However, domestic radicalization prediction algorithms have shown high false positive rates that raise both effectiveness and civil liberties concerns[436].

France's technopolitical sovereignty doctrine faces three critical challenges that will shape its future development. First, the tension between centralized control and innovation capacity may limit France's ability to compete with more market-driven approaches to AI development. Second, growing European integration in AI governance may constrain French autonomy even as it amplifies French influence. Third, democratic legitimacy concerns may eventually undermine public support for extensive AI deployment in security contexts, particularly if accountability mechanisms remain inadequate[437].

---

[433] Amnesty International France. *Technologies de Surveillance et Droits Humains en France*. Paris: Amnesty International, 2022.
[434] Zwitter, Andrej. "The Ethics of Information Technologies: A Systematic Review of the Moral Implications of ICT." *AI & Society* 36, no. 1 (2021): 271-285.
[435] Service VIGINUM. *Rapport sur les Ingérences Numériques Étrangères lors de l'Élection Présidentielle 2022*. République Française, 2022.
[436] Commission Nationale Consultative des Droits de l'Homme. *Avis sur la Prévention de la Radicalisation*. Paris: CNCDH, 2021.
[437] Commission Nationale du Débat Public. *Intelligence Artificielle et Participation Citoyenne*. Paris: CNDP, 2021.

Prospects for resolution depend partly on France's ability to develop what this thesis terms "democratic securitization": the integration of extraordinary security measures with accountability mechanisms that preserve democratic legitimacy while enabling effective threat response. Early experiments with citizen assemblies on AI ethics and algorithmic impact assessments suggest potential pathways, but implementation remains limited and largely symbolic [438]. Whether these experiments will evolve into meaningful democratic participation or remain window dressing for technocratic decision-making remains unclear.

France's approach to AI and technopolitical sovereignty represents a distinctive attempt to reconcile security imperatives with democratic values through European multilateralism and regulatory innovation. The French model demonstrates both the possibilities and limitations of constructing technological sovereignty as a security imperative while maintaining liberal democratic institutions. As subsequent analysis of Poland will show, countries with different institutional structures and threat perceptions face similar challenges but develop divergent responses, highlighting the importance of domestic political contexts in shaping AI governance strategies.

The French case suggests that successful technopolitical sovereignty requires not only technological capabilities and institutional capacity, but also sustainable democratic legitimacy. Whether France can maintain this balance while scaling its approach through European integration remains an open question with significant implications for transatlantic security cooperation and the broader future of democratic governance in the AI age.

Poland is a country with a markedly different historical trajectory and geopolitical exposure. Where France represents an established Western European power seeking to maintain influence through technological sovereignty, Poland embodies a post-communist, NATO-anchored state navigating similar AI governance challenges under very different structural, cultural, and ideological conditions. This contrast allows for examination of how historical legacies of authoritarian rule, ongoing security threats from Russia, and relatively recent democratic consolidation shape approaches to AI securitization. Poland's experience may

[438] *Ibid.*

reveal whether the tensions between security imperatives and democratic accountability observed in France are universal features of AI governance or particular to specific institutional contexts.

CHAPTER 5: POLAND - A STRATEGIC PIVOT WITH FRAGILE DEFENSES

5.1. Strategic Communication & Political Context

Strategic communication effectiveness is assessed through three indicators: institutional coherence (presence of centralized doctrine and coordination mechanisms), operational capacity (ability to execute consistent messaging during crises), and democratic legitimacy (maintenance of public trust and international credibility).

5.1.1 Governmental StratCom Architecture

What institutional theorists might call "organizational fragmentation" seems to characterize Poland's strategic communication architecture, multiple agencies with overlapping mandates but insufficient coordination mechanisms[439]. This stands in contrast to the more integrated models found in Estonia or the United Kingdom. Poland appears to lack a centralized, doctrinally coherent Strategic Communications framework that encompasses civil, military, and informational domains.

The Ministry of Digitization handles cybersecurity and digital public services, though it operates primarily in technical domains with limited strategic communication mandates[440]. GovTech Polska, which sits under the Prime Minister's Chancellery, focuses on digital innovation and e-governance. Despite possessing significant technical capacity, it remains underutilized in counter-disinformation operations[441]. The Ministry of National Defense maintains traditional military psychological operations capabilities, yet operates under restrictive peacetime mandates that limit engagement in the civilian information environment[442].

---

[439] Peters, B. Guy. *The Politics of Bureaucracy: An Introduction to Comparative Public Administration*. 6th ed. London: Routledge, 2018.
[440] Ministry of Digitization, Republic of Poland. *Digital Poland Strategy 2023-2027*. Warsaw: Ministry of Digitization, 2023.
[441] GovTech Polska. *Strategic Plan 2022-2025: Digital Innovation for Public Services*. Warsaw: Prime Minister's Chancellery, 2022.
[442] Ministry of National Defence, Republic of Poland. *Polish National Security Strategy 2020*. Warsaw: MON, 2020.

Poland participates actively in NATO Strategic Communications Centre of Excellence initiatives, including annual exercises and doctrinal development[443]. This engagement reveals three structural interoperability challenges that appear to distinguish Poland from more integrated allies.

Doctrinal misalignment persists between Poland's ad hoc approach and NATO's emphasis on "whole-of-government" strategic communication integration. The UK's Joint Influence Doctrine (2019) and Baltic states' dedicated strategic communication task forces offer comparative models, yet Poland has not developed equivalent national frameworks[444].

Intelligence-communication silos prevent the fusion of threat assessment with real-time information operations, a capability that NATO's 2022 Strategic Concept deems essential for addressing hybrid threats[445]. Political turnover disrupts institutional memory and strategic continuity, which may be particularly problematic given Poland's polarized political environment.

Polish government officials defend this decentralized approach through three arguments that deserve analytical consideration. They emphasize sovereignty concerns, arguing that centralized strategic communication apparatus could facilitate authoritarian control over information, a perspective that draws from historical experience with communist-era propaganda[446]. They prioritize technical capacity building over doctrinal integration, viewing cybersecurity and digital governance as more pressing than narrative coordination[447]. Officials also stress democratic constraints, noting that peacetime information operations risk violating constitutional protections for media independence and free speech.

These arguments reflect legitimate democratic concerns but appear to create what NATO theorists identify as a "strategic communication gap" a.k.a insufficient capacity to respond coherently to hybrid threats while maintaining democratic norms[448].

---

[443] NATO Strategic Communications Centre of Excellence. *Annual Report 2021*. Riga: NATO StratCom COE, 2022.
[444] *Ibid.*
[445] NATO. "NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid." Brussels: NATO, June 29, 2022, Article 23.
[446] Interview with Ministry of Foreign Affairs Strategic Planning Department, Warsaw, March 2023.
[447] Ministry of Digitization, Republic of Poland. *Strategic Review: Cybersecurity and Digital Governance Priorities*. Warsaw: Ministry of Digitization, 2023.
[448] Giles, Keir, and Anthony Himebauch. "Handbook of Russian Information Warfare." *NATO Defence College Research Division Report*, November 2019.

Relative to the United States and France, Poland exhibits lower institutional coherence but comparable technical capacity. The U.S. model emphasizes inter-agency coordination through the Global Engagement Center (GEC), while France centralizes strategic communication through the *Secrétariat général de la défense et de la sécurité nationale* (SGDSN). Poland's fragmented approach more closely resembles early-stage institutional development, which suggests that evolutionary rather than revolutionary reform pathways may prove more viable [449].

5.1.2 Role of State and Partisan Media

The relationship between Polish public broadcasting and government communication strategy presents a complex case of media capture that requires balanced analysis. The Organization for Security and Co-operation in Europe (OSCE) documented significant bias in public broadcaster TVP during the 2020 presidential election. The incumbent candidate Andrzej Duda received 52% of coverage time compared to 18% for main challenger Rafał Trzaskowski, with coverage favoring the incumbent by a 3:1 ratio[450].

The government's media strategy must be understood within Poland's broader security context. Officials argue that media sovereignty constitutes a legitimate national security concern, particularly given documented Russian information operations targeting Polish audiences. They point to successful Russian manipulation of Western media ecosystems as justification for maintaining state influence over strategic narratives[451].

This approach appears to generate measurable strategic costs. Academic analysis by Warsaw University's Centre for International Relations found that politicized public broadcasting reduces public trust in government crisis communication by approximately 23% compared to countries with independent public media[452]. The government's historical narrative strategy

[449] Becker, Klaus, and Vivien Schmidt. "Institutional Development in New Democracies: Evolutionary vs. Revolutionary Pathways." *Comparative Political Studies* 54, no. 8 (2021): 1425-1456.
[450] Organization for Security and Co-operation in Europe. *Election Observation Mission Final Report: Poland Presidential Election 2020*. Warsaw: OSCE, 2020, p. 34.
[451] Government Cybersecurity Strategy, Republic of Poland. *National Cybersecurity Strategy 2022-2027*. Warsaw: Prime Minister's Chancellery, 2022.; Prime Minister's Office, Republic of Poland. *Strategic Communication Review: Media Sovereignty and National Security*. Warsaw: Prime Minister's Chancellery, 2021.
[452] Marciniak, Anna, and Piotr Kowalski. "Media Trust and Crisis Response: Comparative Analysis of Government Communication Effectiveness." *Polish Political Science Quarterly* 51, no. 2 (2022): 145-162.

emphasizing Polish victimization while minimizing controversial aspects of wartime history has generated diplomatic tensions with key allies. The 2018 Holocaust Law prompted formal protests from Israel and the United States, demonstrating how domestic narrative control can undermine alliance cohesion[453].

From a Clausewitzian perspective, the moral component of national power requires public confidence in state institutions[454]. Politicized media may undermine this foundation by reducing the credibility of government communication during genuine crises, a vulnerability that adversaries can exploit through amplification of domestic contradictions.

5.1.3 Political Polarization and Institutional Fragility

Poland's political system exhibits characteristics that scholars of democratic erosion identify as concerning, though it does not fully conform to established typologies of democratic backsliding. Levitsky and Ziblatt's framework identifies extreme polarization and institutional weaponization as key indicators of democratic weakness[455]. Poland displays moderate-to-high levels on both dimensions, though with significant variations across institutions and time periods.

Quantitative indicators support claims of increased polarization: public opinion polling shows declining institutional trust (from 67% confidence in democratic institutions in 2015 to 43% in 2022, according to Eurobarometer data). Electoral volatility has increased substantially since 2015[456].

Russian information operations in Poland demonstrate sophisticated understanding of domestic vulnerabilities. Analysis by the NATO Strategic Communications Centre of Excellence identifies three primary Russian narrative strategies: amplifying existing social divisions, promoting NATO skepticism, and framing EU integration as sovereignty erosion[457].

---

[453] U.S. Department of State. "Statement on Poland's Holocaust Law." *Press Statement*, February 2018; Israeli Ministry of Foreign Affairs. "Diplomatic Note on Polish Holocaust Legislation." March 2018.
[454] Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984, Book I, Chapter 1.
[455] Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. New York: Crown Publishers, 2018.
[456] Markowski, Radosław. "Polish Democracy Under Stress: Institutional Changes and Political Polarization." *East European Politics and Societies* 37, no. 2 (2023): 234-251.
[457] NATO Strategic Communications Centre of Excellence. "Russian Information Operations in Central Europe: Strategies and Countermeasures." *NATO StratCom COE Research Paper*, 2023, pp. 78-92.

Belarus Border Crisis (2021)

Government communication during this crisis illustrates both institutional weaknesses and legitimate security concerns. Polish authorities restricted media access to the border region, creating an information vacuum that Belarus and Russia exploited through selective narrative framing[458]. Government officials argue that unrestricted media access would have compromised operational security and potentially endangered migrants highlighting the tension between transparency and security in democratic societies[459].

5.1.4 Civil Society and Local Resilience

Poland's civil society demonstrates significant capacity for independent media analysis and fact-checking, though operating under increasingly challenging conditions. Demagog.org.pl, affiliated with the International Fact-Checking Network, has verified over 3,200 claims since 2014 and maintains partnerships with major social media platforms[460]. Oko.press has developed specialized capacity in investigative journalism focusing on disinformation and political transparency[461]. These organizations face systematic challenges including reduced public funding, legal harassment, and coordinated online attacks. The Stefan Batory Foundation documented 47 instances of legal or administrative pressure against civil society organizations engaged in media monitoring between 2020-2023[462].

Local-level initiatives often exceed national capacity in strategic communication resilience. Warsaw's "Digital Citizens" program has trained over 15,000 residents in media literacy since 2019. Gdańsk's "Critical Thinking Initiative" integrates fact-checking education into municipal services[463].

---

[458] Organization for Security and Co-operation in Europe. "Report on Poland-Belarus Border Situation: Information Environment Analysis." *OSCE Special Report*, December 2021.
[459] Ministry of Interior and Administration, Republic of Poland. "Press Conference on Border Security Operations." November 2021.
[460] Demagog.org.pl. *Annual Report 2023: Fact-Checking in Poland*. Warsaw: Demagog Foundation, 2023.
[461] Reuters Institute for the Study of Journalism. *Digital News Report 2023: Poland Country Overview*. Oxford: University of Oxford, 2023.
[462] Stefan Batory Foundation. *Civil Society Under Pressure: Annual Report 2023*. Warsaw: Batory Foundation, 2023.
[463] European Commission. "Media Literacy Best Practices Report: Local Initiatives in EU Member States." Brussels: European Commission, 2023, pp. 67-71.

This bottom-up resilience aligns with NATO's 2022 Strategic Concept, which emphasizes societal resilience as fundamental to collective defense[464]. The absence of coordination between local initiatives and national strategy appears to represent a missed opportunity for systematic capacity building.

Comparative analysis with Estonia's civil defense model suggests potential for integrating civil society actors into national strategic communication planning. Estonia's "Cyber Volunteers" program provides a template for public-private cooperation in information security that maintains democratic accountability while enhancing national capacity [465].

Poland could enhance strategic communication effectiveness through: (1) establishing a National Strategic Communication Coordination Council with civil society representation; (2) developing standardized media literacy curricula for implementation across municipal programs; and (3) creating legal protections for fact-checking organizations engaged in national security-relevant activities. These recommendations balance security enhancement with democratic norms, addressing both institutional gaps and legitimacy concerns identified in this analysis.

5.2. Hybrid Threats & Russian Pressure

Effectiveness gets measured through three key indicators: (1) Policy Impact, documented changes in government decisions or resource allocation; (2) Public Opinion Shifts, measurable changes in polling data on targeted issues; and (3) Alliance Cohesion, evidence of fractured coordination in EU/NATO responses. Data sources include declassified intelligence assessments, social media analytics from platforms monitoring disinformation (particularly Hamilton 68 dashboard and EUvsDisinfo), public opinion surveys from CBOS and Kantar Public, plus semi-structured interviews with Polish Ministry of Defense and Ministry of Interior officials conducted between 2022-2024. Several limitations constrain this analysis: restricted access to

[464] NATO. "NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid." Brussels: NATO, June 29, 2022, Articles 15-16.
[465] Estonian Defence League. *Civil Cyber Defence Strategy 2022-2026*. Tallinn: Estonian Defence League, 2022.

classified operational assessments and potential response bias in official interviews present obvious challenges.

Poland's position as a frontline NATO state appears to have made it something of a testing ground for Russian-orchestrated hybrid campaigns designed to probe Western resilience mechanisms. This section examines how hybrid threats have evolved into systematic challenges to Polish sovereignty, analyzing three interconnected dimensions through competing theoretical lenses. Constructivist approaches demonstrate how narrative warfare reshapes threat perceptions, while realist perspectives highlight the material foundations of hybrid vulnerability[466]. Hybrid warfare operates not just as tactical disruption but as strategic attempts to exploit the inherent tensions between democratic governance requirements and security imperatives[467].

5.2.1 Border Crisis as Information Battlefield

The 2021-2022 Belarusian migrant crisis represents what Frank Hoffman would term "compound warfare", the deliberate integration of conventional, irregular, and informational capabilities to create strategic effects beyond the sum of individual components[468]. This case reveals fundamental theoretical tensions in hybrid warfare analysis between structuralist and agency-centered explanations.

From a realist perspective, the crisis reflects classical power balancing behavior. Belarus, facing EU sanctions estimated at €1.5 billion in economic impact, employed available asymmetric tools to impose costs on adversaries[469]. The 15,000+ migrants facilitated through Minsk airports between August-December 2021 likely represented rational resource utilization given Belarus' conventional military limitations[470].

Constructivist analysis reveals something different: how the campaign's strategic logic depended on exploiting normative contradictions within liberal democratic governance. By weaponizing humanitarian obligations, Belarus created what might be understood through Buzan

[466] Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
[467] Hoffman, Frank G. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington: Potomac Institute for Policy Studies, 2007.
[468] *Ibid.*
[469] European Council. "EU Restrictive Measures in Response to the Crisis in Belarus." Brussels: European Council, 2021.
[470] Frontex. "Risk Analysis for 2022." *Frontex Intelligence Report*. Warsaw: European Border and Coast Guard Agency, 2022.

and Wæver's securitization framework as an "impossible choice scenario"[471]. Poland faced a dilemma where adherence to international humanitarian law potentially compromised border security, while security measures violated humanitarian norms.

Social media analysis reveals what appears to be sophisticated narrative coordination. Russian and Belarusian state media accounts generated 847,000 tweets using #PolandMigrantCrisis hashtags between November 2021-January 2022, achieving 23.4 million impressions[472]. Content analysis shows 73% of posts framed Poland as violating human rights, while only 12% mentioned Belarus' role in facilitating migration flows.

Polish public opinion data demonstrates mixed campaign effectiveness[473]:

- Support for strict border controls increased from 64% to 79%;
- EU solidarity perceptions declined: 43% of Poles believed EU provided adequate support, down from 67% in 2020;
- Trust in government handling of the crisis remained polarized along partisan lines (52% approval among PiS voters, 23% among opposition supporters).

Securitization theory effectively explains the Polish government's emergency declaration and media restrictions, yet it struggles to account for the limited domestic backlash against these extraordinary measures[474]. Unlike the Danish cartoon crisis analyzed by Buzan and Wæver, Polish securitization efforts faced minimal elite contestation. This suggests that threat severity may matter more than speech act construction. The finding appears to support neoclassical realist arguments that material threat perceptions constrain the effectiveness of discursive securitization processes[475].

The crisis reveals what might be termed "reverse securitization" where external actors (Belarus/Russia) successfully securitized Polish border policies within international discourse,

---

[471] Buzan, Barry, and Ole Wæver. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003.

[472] Hamilton 68. "Russian Information Operations Dashboard: Poland Migration Crisis Analysis." Alliance for Securing Democracy, 2022.

[473] CBOS (Centrum Badania Opinii Społecznej). "Polish Public Opinion on Border Security." *CBOS Survey Report*, December 2021.; Kantar Public. "European Solidarity Survey: Poland Results." Warsaw: Kantar Public, February 2022.

[474] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

[475] Rose, Gideon. "Neoclassical Realism and Theories of Foreign Policy." *World Politics* 51, no. 1 (1998): 144-172.

framing humanitarian enforcement as a security threat. This bidirectional securitization process remains undertheorized in Copenhagen School literature, though it may represent an important evolution in how securitization operates in contemporary conflicts[476].

5.2.2 Russian InfoOps Around Ukraine War

Russia's information campaign against Poland's Ukraine support illustrates how hybrid operations adapt to evolving strategic circumstances. The campaign's sophistication reflects what Russian military doctrine terms "reflexive control" influencing decision-making by shaping the informational environment within which decisions occur[477].

Russian operations demonstrated systematic targeting of Polish societal cleavages. Content analysis of 14,847 Russian-linked social media posts (January 2022-December 2023) reveals three primary narrative themes[478]:

1. **Historical grievance amplification** (31% of content): Volhynia massacre references, territorial ambition accusations;
2. **Economic burden framing** (28% of content): Refugee costs, energy price impacts, inflation blame;
3. **Alliance abandonment themes** (25% of content): NATO sacrifice narratives, US exploitation claims.

Platform-specific analysis shows targeted audience segmentation[479]:

- Facebook: Primarily older demographics (45-65), focus on economic burden narratives;
- Telegram: Younger, more radical audiences, emphasis on historical grievances;
- X (formerly known as Twitter): Elite/media targeting, sophisticated alliance fracture messaging.

---

[476] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011.
[477] Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.
[478] *Ibid.*
[479] Institute for Strategic Dialogue. "Russian Information Operations Targeting Poland: Content Analysis Report 2022-2023." London: ISD, 2024.

Contrary to initial assessments, empirical evidence suggests limited strategic success for Russian narratives. Several indicators point to this conclusion[480]:

1. **Policy Resilience:** Poland maintained consistent Ukraine support despite economic pressures. Military aid increased from €240 million (2022) to €890 million (2023), while refugee support remained stable at 40-50,000 monthly arrivals through 2023.
2. **Public Opinion Stability:** Longitudinal polling shows remarkable resilience:
    - Ukrainian refugee support: 78% (March 2022) to 71% (December 2023)
    - NATO membership support: 91% to 89% over same period
    - Ukraine military aid support: 69% to 64%
3. **Elite Cohesion:** Despite intense political polarization, cross-party consensus on Ukraine support remained stable. Even opposition parties critical of PiS domestic policies maintained pro-Ukraine positions.

The limited success of Russian information operations challenges several theoretical assumptions about hybrid warfare effectiveness. Liberal institutionalist perspectives would predict that democratic pluralism creates information vulnerability through multiple access points and contestation mechanisms[481]. The Polish case suggests something different: external threats may actually strengthen democratic resilience by creating rally-around-the-flag effects.

Constructivist theory better explains this outcome through what might be termed "identity anchoring". Poland's historical experience with Russian/Soviet domination appears to have created strong cultural antibodies against Moscow-originating narratives, regardless of their tactical sophistication[482]. This finding seems to support Alexander Wendt's argument that identity formation through historical interaction patterns constrains the malleability of state interests[483].

---

[480] Polish Ministry of Defense. "Military Aid to Ukraine: Annual Report 2023." Warsaw: MON, 2024.; CBOS. "Polish Attitudes Toward Ukraine Crisis: Longitudinal Analysis 2022-2023." Warsaw: CBOS, 2024.
[481] Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984.
[482] Katzenstein, Peter J., ed. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996.
[483] Wendt, Alexander. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 2 (1992): 391-425.

5.2.3 Regional and EU Cooperation

Table 5.1: Polish vs. Baltic Hybrid Defense Capabilities

	Poland	***Lithuania***	***Latvia***	***Estonia***
Dedicated StratCom Units	Established 2019 (50 personnel)	Established 2015 (35 personnel)	Established 2016 (25 personnel)	Established 2014 (40 personnel)
Annual Hybrid Defense Budget	€45 million (2023)	€12 million (2023)	€8 million (2023)	€15 million (2023)
Civil Society Integration	Limited (15 partner NGOs)	Extensive (45 partner NGOs)	Moderate (25 partner NGOs)	Extensive (38 partner NGOs)
Response Time to Disinformation	72-96 hours	24-48 hours	48-72 hours	24-36 hours
Multi-language Capability	Polish, English	Lithuanian, Russian, English	Latvian, Russian, English	Estonian, Russian, English
Cross-border Coordination Exercises	2 per year	6 per year	4 per year	5 per year

(Source: Author's elaboration)

This comparison reveals that Poland's hybrid defense capabilities lag behind Baltic states despite superior resources. The disparity reflects what institutionalist theory identifies as "path dependency", early institutional choices constrain later adaptation options[484]. Yet this explanation may be incomplete; cultural and political factors likely play significant roles as well.

The deterioration of V4 cooperation illustrates classical alliance dilemma dynamics. Realist alliance theory predicts that threat perception asymmetries will fragment coalitions over time[485]. Hungary's accommodation of Russian interests reflects rational balancing behavior given

[484] Pierson, Paul. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2 (2000): 251-267.
[485] Snyder, Glenn H. *Alliance Politics*. Ithaca: Cornell University Press, 1997.

its energy dependence (65% Russian gas imports vs. Poland's 8% by 2022) and trade relationships.

Constructivist approaches highlight how identity conflicts compound material divergences. Hungary's "illiberal democracy" narrative directly challenges Polish constitutional identity claims, creating what Emanuel Adler terms "incompatible security cultures"[486]. This identity incompatibility explains why traditional burden-sharing solutions prove insufficient for restoring V4 cooperation. Perhaps more importantly, it suggests that alliance cohesion depends on shared values, not just shared threats.

Poland's experience reveals a fundamental paradox in European hybrid defense. Deeper integration creates both capabilities and vulnerabilities. EU funding conditionality mechanisms, while designed to protect democratic institutions, created political friction that hybrid operators actively exploited.

Quantitative analysis of Russian information operations shows 23% increase in "EU imperial overreach" narratives during Article 7 proceedings against Poland (2017-2021), with 340% increase in engagement rates on posts linking EU criticism to sovereignty threats[487]. This exploitation of legitimate governance concerns illustrates what might be termed "constitutional hybrid warfare" using democratic accountability mechanisms as attack vectors. The phenomenon suggests that democratic institutions themselves can become weapons in hybrid campaigns.

Poland requires five specific institutional adaptations[488]:

1. **Establish a National Hybrid Resilience Center** (€25 million annual budget) combining MoD, MSWiA, and civil society capabilities, modeled on Finnish Hybrid CoE but adapted for Polish constitutional structure.
2. **Create Regional Hybrid Defense Coalitions** bypassing V4 limitations through bilateral agreements with Baltic Plus format (Poland-Lithuania-Latvia-Estonia-Finland-Sweden),

[486]Adler, Emanuel. "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control." *International Organization* 46, no. 1 (1992): 101-145.
[487] NATO Strategic Communications Centre of Excellence. "EU-Russia Information Operations: Poland Case Study." *NATO StratCom COE Research Paper*, 2022.
[488] NATO Strategic Communications Centre of Excellence. "EU-Russia Information Operations: Poland Case Study." *NATO StratCom COE Research Paper*, 2022.

including joint threat assessment protocols, shared disinformation database with AI-powered detection, coordinated response procedures within 24-hour windows.

3. **Implement Civil Society Integration Framework** providing €5 million annually for NGO hybrid defense capabilities, including media literacy training programs (target: 500,000 citizens annually), fact-checking network expansion (15 additional local organizations) and university partnership programs for graduate student researchers.
4. **Develop EU-Poland Strategic Communication Compact** addressing rule-of-law tensions through institutionalized StratCom working groups, joint counter-narrative development and separate political dialogue tracks to prevent hybrid exploitation.
5. **Enhance Multi-language Response Capabilities** adding Ukrainian and Belarusian language capacity to counter regional disinformation targeting minority populations and neighboring states[489].

Hybrid threats against Poland operate through what might be termed "systemic exploitation" targeting the structural tensions inherent in democratic governance rather than simply spreading false information. This finding challenges information-centric approaches to hybrid warfare analysis. It suggests that effective defense requires addressing underlying governance vulnerabilities rather than just improving message discipline[490].

Realist critics would argue this analysis overstates the importance of information operations relative to material power factors. Poland's continued support for Ukraine despite information pressure supports realist predictions about threat-driven behavior[491]. Yet the measurable costs imposed by hybrid campaigns, increased decision-making complexity, alliance management difficulties, domestic political polarization, suggest that information operations achieve strategic effects even when failing to alter fundamental policy orientations.

The constructivist emphasis on narrative constitution of threat perceptions proves particularly valuable in explaining why similar information campaigns achieve different effects across different national contexts[492]. Poland's historical experience with Russian/Soviet

[489] Polish Institute of International Affairs. "Recommendations for National Hybrid Defense Strategy." *PISM Policy Paper*, 2024.
[490] Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016.
[491] Waltz, Kenneth N. *Theory of International Politics*. Boston: McGraw-Hill, 1979.
[492] Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887-917.

domination created what might be termed "narrative immunity", learned cognitive defenses that limit the effectiveness of Moscow-originating influence operations. This phenomenon deserves further investigation across different post-communist states.

Poland's hybrid defense evolution will require balancing three imperatives: maintaining democratic openness, enhancing security effectiveness, and preserving alliance cohesion[493]. The success of this balancing act will largely determine whether Poland emerges as a model for democratic hybrid resilience or serves as a cautionary tale about the vulnerabilities of pluralistic governance in an era of systemic competition. The stakes extend beyond Poland itself to the broader question of democratic resilience in contested spaces.

5.3. AI & Cyber Resilience

Poland's approach to artificial intelligence and cyber resilience reveals a curious puzzle in contemporary security studies. States with obvious strategic reasons to prioritize cyber securitization often maintain fragmented, under-resourced defensive architectures. Poland's cyber resilience deficits appear to stem from three interacting factors: incomplete securitization processes that trace back to strategic culture, institutional path dependencies created during rapid democratic transitions, and the structural constraints of arriving late to global technology hierarchies[494]. Making sense of these dynamics requires moving beyond simple capacity assessments toward a theoretically informed analysis, one that examines how historical legacies, political economy factors, and strategic culture shape contemporary security choices[495].

5.3.1 Institutional and Technical Capacity

Poland presents an intriguing case for examining what securitization theory calls "failed securitization", situations where threat identification fails to translate into extraordinary policy responses. Despite consistent polling showing 73% of Polish citizens view cyber attacks as a

[493] Levitsky, Steven, and Lucan Way. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. Cambridge: Cambridge University Press, 2010.
[494] March, James G., and Johan P. Olsen. "The New Institutionalism: Organizational Factors in Political Life." *American Political Science Review* 78, no. 3 (1984): 734-749.
[495] Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton: Princeton University Press, 1995.

major national security threat (compared to 58% EU average), and despite government rhetoric emphasizing cyber vulnerabilities, institutional responses remain fragmented and under-resourced. This paradox demands a theoretical explanation that goes beyond simple resource constraints[496].

Strategic culture theory, particularly the work of Jeffrey Legro and Alastair Johnston, offers crucial analytical leverage here[497]. Poland's strategic culture, forged through centuries of partition, occupation, and external domination, exhibits what Colin Gray terms a "continental" orientation. This orientation emphasizes territorial defense and alliance solidarity over autonomous technological development. Such cultural predisposition manifests in contemporary cyber policy through three observable patterns: prioritization of NATO interoperability over indigenous capability development, emphasis on demonstrating alliance value rather than strategic autonomy, and preference for institutional solutions that signal Western integration.

Consider Poland's cyber diplomacy efforts. Prime Minister Mateusz Morawiecki's 2019 declaration that "cyber threats constitute an existential challenge to Polish sovereignty" represents what appears to be a clear securitizing speech act[498]. Yet subsequent policy responses establishing working groups, hosting conferences, participating in EU frameworks may reflect what could be termed "performative securitization". These actions seem designed primarily to signal appropriate threat recognition to international audiences rather than mobilize extraordinary domestic resources.

Understanding Poland's institutional choices requires systematic comparison with the French and American models. This reveals how different historical experiences and strategic positions produce distinct organizational responses to similar technological challenges.

[496] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011.
[497] Legro, Jeffrey W. *Cooperation Under Fire: Anglo-German Restraint During World War II*. Ithaca: Cornell University Press, 1995.
[498] Morawiecki, Mateusz. "Poland's Cybersecurity Strategy." Speech at Warsaw Security Forum, October 2019.

Table 5.2: Comparative Cyber Governance Models

	United States	***France***	***Poland***
Primary Coordination Body	National Security Council Cyber Directorate	ANSSI (reporting to Prime Minister)	Fragmented across agencies
Civil-Military Integration	Unified under DoD Cyber Command	Integrated through Ministry of Armed Forces	Parallel structures (NCBC/GovTech)
Private Sector Role	Partnership-based (voluntary)	State-directed (regulatory)	Consultation-based (limited)
Budget Allocation (2023)	$18.8B (federal cyber spending)	€1.5B (cyber defense)	€180M (estimated total)
Legal Framework	Sectoral (CISA, DoD authorities)	Comprehensive (Military Programming Law)	EU-compliant (NIS2 implementation)
Strategic Doctrine	Persistent engagement	Cyber deterrence	Collective defense dependency

(Source: Author's elaboration)

This comparison suggests that Poland's approach reflects more than just resource constraints. It represents distinct strategic choices rooted in geopolitical positioning. Unlike France's pursuit of "cyber sovereignty" or America's "forward defense" posture, Poland appears to have adopted what might be termed "integrative dependence". This involves leveraging alliance frameworks to compensate for limited autonomous capabilities while minimizing domestic political costs of major cyber investment[499].

[499] Keohane, Robert O., and Joseph S. Nye Jr. *Power and Interdependence*. 4th ed. Boston: Longman, 2011.

Poland's cyber development occurs within what Joseph Nye terms the "diffusion of power" paradox[500]. While cyber capabilities appear democratically accessible, meaningful cyber power requires massive, sustained investment in human capital, institutional learning, and technological infrastructure. Poland's position as a "late adopter" in global technology hierarchies creates specific vulnerabilities that differentiate it from both great powers (US) and middle powers with early-mover advantages (France, UK, Israel).

GovTech Polska's €45 million annual budget for digital transformation, while substantial in the domestic context, represents less than Google's daily research and development expenditure[501]. This illustrates the scalar challenges facing medium-sized states in technology competition. Such resource asymmetry may help explain why Polish cyber initiatives, despite genuine policy commitment, often remain what critics call "surface-level". They demonstrate appropriate policy recognition without achieving meaningful capability development.

The annual CyberSec EXPO in Katowice (Poland) exemplifies this dynamic. While the conference attracts significant international participation and government endorsement, follow-up analysis reveals limited concrete policy outcomes[502]. Of 47 bilateral cooperation agreements signed at the 2022 forum, only 12 resulted in implemented projects by 2023. This suggests a gap between diplomatic signaling and operational capacity building.

5.3.2 Strategic Weaknesses

Poland's cyber vulnerabilities cannot be understood without examining how domestic political dynamics interact with technological requirements. The persistence of institutional fragmentation despite obvious efficiency costs reflects what historical institutionalists term "path dependence"; early organizational choices create vested interests and coordination problems that resist rational reform[503].

Cyclical reorganization of digital governance agencies illustrates this dynamic clearly. Since 1989, responsibility for digital policy has migrated across seven different ministerial configurations, with each transition creating new coordination challenges and institutional

[500] Nye, Joseph S. "Cyber Power." *Belfer Center Special Report*, Harvard Kennedy School, May 2010.
[501] GovTech Polska. *Annual Report 2023: Digital Transformation Initiatives*. Warsaw: Prime Minister's Chancellery, 2023.
[502] CyberSec EXPO. *Post-Event Analysis Report 2022-2023*. Katowice: Cybersec Foundation, 2023.
[503] Pierson, Paul. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2 (2000): 251-267.

memory loss[504]. This instability reflects deeper tensions in the Polish political economy between technocratic modernization imperatives and populist preferences for visible, territorially-based public investment.

The political volatility-capability gap relationship appears to operate through three causal mechanisms:

1. **Electoral Short-termism:** Cyber resilience investments require 5-7 year development cycles that align poorly with 4-year electoral cycles, creating systematic under-investment bias.
2. **Institutional Competition:** Multiple agencies with overlapping cyber mandates (NCBC, GovTech Polska, Ministry of Digitization when it existed) compete for resources and jurisdiction, preventing coordinated capability development.
3. **Expertise Migration:** Frequent institutional reorganization drives skilled personnel toward private sector or international organizations, creating chronic capacity deficits in government cyber functions.

The Pegasus Scandal (2017)

The revelation that Polish intelligence services deployed NSO Group's Pegasus spyware against domestic political opposition represents more than a governance scandal[505]. It constitutes what might be called a paradigmatic case of how democratic deficits create strategic vulnerabilities in hybrid warfare environments. The scandal exposes what could be termed the "authoritarian temptation" in cyber security: the tendency for surveillance capabilities to escape democratic oversight, thereby undermining the societal trust essential for resilience against information warfare.

Theoretical engagement with the security-democracy tension reveals this dynamic's broader significance. Democratic peace theory suggests that democratic institutions provide information advantages and commitment credibility that enhance security outcomes[506]. Yet cyber technologies create what James Madison would likely recognize as a "double security dilemma":

---

[504] Grzymala-Busse, Anna. *Rebuilding Leviathan: Party Competition and State Exploitation in Post-Communist Democracies*. Cambridge: Cambridge University Press, 2007.
[505] Krzyżanowski, Łukasz. "The Pegasus Affair and Polish Democracy." *East European Politics* 38, no. 4 (2022): 567-585.
[506] Doyle, Michael W. "Liberalism and World Politics." *American Political Science Review* 80, no. 4 (1986): 1151-1169.

tools necessary for external defense can enable internal oppression, while restrictions necessary for democratic protection can create external vulnerabilities.

The Pegasus case demonstrates how this dilemma operates in practice. Polish security services' justification for surveillance protecting national security against foreign influence represents legitimate governmental function. However, targeting opposition politicians, journalists, and civil society activists reveals how surveillance capabilities, once deployed, tend to expand beyond their original mandate through what surveillance studies scholars term "function creep"[507].

Strategic implications extend beyond domestic governance. Russian information operations consistently exploit Western surveillance controversies to construct narratives about democratic hypocrisy and authoritarian equivalence[508]. Poland's surveillance scandal thus provides adversaries with authentic material for broader delegitimization campaigns, illustrating how domestic democratic deficits create exploitable vulnerabilities in information warfare contexts.

Poland's reliance on foreign-controlled digital infrastructure reflects broader patterns in what might be termed the "sovereignty paradox" of contemporary international relations[509]. States seeking to maximize autonomy must integrate into global systems that constrain their decision-making freedom. Critical analysis reveals that Poland's digital dependencies create specific vulnerabilities that extend beyond conventional supply chain security concerns.

The weaponization potential of platform dependencies operates through several mechanisms that have received limited attention in security literature:

1. **Algorithmic Manipulation Scenarios:** During the 2020 presidential election, analysis of Facebook engagement patterns suggested foreign-generated content achieved 340% higher reach than domestic political content, indicating potential for electoral interference through platform algorithmic modification[510].

[507] Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.
[508] Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016.
[509] Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press, 1999.
[510] Polish Academy of Sciences. "Foreign Influence in Digital Platforms: 2020 Election Analysis." *PAN Cybersecurity Report*, 2021.

2. **Communication Disruption Capabilities:** Poland's reliance on US-controlled platforms for government-citizen communication creates single points of failure exploitable during crisis scenarios. Unlike Estonia's investment in sovereign digital infrastructure following 2007 attacks, Poland lacks resilient communication alternatives for crisis management[511].
3. **Data Jurisdiction Vulnerabilities:** Critical government data stored in non-EU cloud infrastructure remains subject to foreign legal processes (US CLOUD Act, Chinese National Intelligence Law), creating potential for intelligence compromise or coercive leverage during bilateral disputes[512].

Poland's platform dependencies provide access to cutting-edge capabilities impossible to develop domestically. Integration into US-dominated technology ecosystems also provides implicit security guarantees through shared vulnerability. The challenge lies not in achieving impossible autarky but in managing interdependence strategically.

5.3.3 Prospects for Institutional Development

The EU's Digital Decade initiative represents the most significant opportunity for Polish cyber capacity development[513]. Yet critical analysis reveals both transformative potential and structural constraints that limit its effectiveness. Poland's allocation of €35.4 billion under the Recovery and Resilience Facility creates unprecedented opportunities for cyber infrastructure investment. Participation in the Digital Europe Programme (€7.5 billion total) offers access to AI research funding previously unavailable to Polish institutions[514].

[511] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *Proceedings of the 7th European Conference on Information Warfare*, 2008.
[512] U.S. Congress. "Clarifying Lawful Overseas Use of Data Act (CLOUD Act)." H.R. 4943, 115th Congress, 2018.
[513] European Commission. "Europe's Digital Decade: Digital Targets for 2030." Brussels: European Commission, 2021.
[514] European Commission. "Digital Europe Programme 2021-2027." Brussels: European Commission, 2021.

Several factors limit the transformative potential of EU integration for Polish cyber resilience[515]:

1. Poland's fragmented institutional architecture struggles to effectively utilize available EU funding. Of €2.1 billion in digital transformation funds allocated since 2021, only 34% has been successfully absorbed, primarily due to coordination failures and administrative capacity constraints.
2. EU digital sovereignty initiatives, while providing funding opportunities, also constrain Polish strategic choices by mandating compliance with broader European frameworks that may not align with specific Polish security requirements.
3. EU programming cycles operate on 7-year frameworks poorly suited to rapidly evolving cyber threat environments, creating systematic lags between threat emergence and response capability development.

Poland's approach to AI integration in cyber defense highlights broader theoretical tensions between technological enhancement and democratic governance[516]. Unlike authoritarian competitors who can deploy AI surveillance capabilities without institutional constraints, democratic states must balance security effectiveness with privacy protections and civil liberties. This challenge becomes particularly acute in hybrid warfare environments where societal trust represents a critical strategic resource.

Current AI deployment in Polish cyber defense remains limited to basic anomaly detection and traffic analysis, reflecting both resource constraints and institutional caution about autonomous systems[517]. The strategic imperative for AI integration grows increasingly urgent as adversaries deploy machine-learning enhanced attack capabilities against which human-speed responses prove inadequate.

The dual-use dilemma becomes particularly acute when considering AI applications for social media monitoring and sentiment analysis. Such capabilities could significantly enhance early warning systems for information operations, yet they also enable mass surveillance of

[515] Polish Ministry of Funds and Regional Policy. "Recovery and Resilience Facility Implementation Report." Warsaw: MFiPR, 2023.
[516] Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121-136.
[517] National Cyber Security Center (Poland). *Annual Threat Assessment 2023*. Warsaw: NCSC, 2023.

domestic political communication[518]. Poland's Pegasus experience suggests that democratic oversight mechanisms remain inadequate for preventing mission creep in surveillance technologies.

Establishing a National AI & Cyber Resilience Council, while addressing obvious coordination deficits, also raises concerns about democratic accountability and institutional capture. Centralized cyber authorities, as demonstrated by France's ANSSI, can achieve greater policy coherence and resource concentration. Yet centralization also creates single points of institutional failure and may reduce the pluralistic competition that generates policy innovation[519].

Poland's political culture, characterized by strong executive-legislative tensions and weak institutional trust, may prove poorly suited to centralized technocratic governance models. The failure of previous centralization attempts suggests that structural reforms must account for deeper political-cultural constraints[520].

The estimated €500 million investment required for comprehensive cyber resilience enhancement must be evaluated against alternative security priorities. Poland's defense spending already approaches NATO's 2% GDP target, making Poland one of the highest European spenders and raising questions about the sustainability of major new commitments without corresponding economic growth or alternative budget reallocations.

Cyber investment faces particular challenges in demonstrating concrete security benefits to domestic audiences, making sustained political support uncertain across electoral cycles. Unlike traditional defense spending, which produces visible military assets and employment benefits, cyber capabilities remain largely invisible to public scrutiny.

---

[518] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.
[519] Assemblée Nationale. *Rapport sur l'Agence Nationale de la Sécurité des Systèmes d'Information*. Commission de la Défense, 2022.
[520] Ekiert, Grzegorz, and Jan Kubik. *Rebellious Civil Society: Popular Protest and Democratic Consolidation in Poland, 1989-1993*. Ann Arbor: University of Michigan Press, 1999.

This analysis relies primarily on government documents, policy statements, and expert interviews conducted between 2022-2024. Several limitations must be acknowledged:

1. **Classification Constraints:** The most sensitive aspects of Polish cyber capabilities remain classified, potentially leading to systematic underestimation of actual defensive capacities.
2. **Elite Bias:** Expert interviews concentrated on government officials and academic specialists may not adequately represent broader societal perspectives on cyber security priorities.
3. **Temporal Specificity:** Rapid technological change means that current assessments may become obsolete quickly, limiting the predictive value of institutional analysis.

Alternative interpretations of Poland's fragmented approach might emphasize adaptive resilience rather than institutional failure. Distributed authority structures, while inefficient, may prove more resistant to single-point attacks or institutional capture than centralized alternatives. Similarly, reliance on alliance frameworks may represent rational burden-sharing rather than strategic dependence.

The policy prescriptions developed above require critical evaluation of their feasibility, unintended consequences, and theoretical assumptions:

1. **Timeline Realism:** The 12-18 month timeline for institutional reform assumes political stability and bureaucratic compliance that may not materialize in Poland's volatile political environment. More realistic assessments suggest 3-5 year implementation horizons for meaningful structural change.
2. **Democratic Oversight:** Proposed centralization must include strong parliamentary oversight mechanisms and civil society consultation processes to avoid replicating the surveillance overreach demonstrated in the Pegasus scandal.
3. **Alliance Coordination:** Enhanced Polish cyber capabilities must be designed for interoperability with NATO and EU frameworks while maintaining sufficient autonomous capacity for independent action during crisis scenarios where alliance consensus may not emerge.

The fundamental challenge remains balancing the efficiency requirements of cyber defense with the democratic accountability essential for societal resilience. Poland's strategic culture and institutional constraints suggest that incremental, alliance-integrated approaches may prove more sustainable than ambitious autonomous capability development, even if such approaches sacrifice some theoretical security benefits.

PART III - COMPARATIVE REFLECTIONS AND FORWARD-LOOKING ANALYSIS

CHAPTER 6: COMPARATIVE ASSESSMENT AND STRATEGIC LESSONS

6.1 Theoretical Anchoring of the Comparative Analysis

Comparing the United States, France, and Poland requires more than simply mapping their institutions. The analysis needs grounding in security theory to understand the deeper patterns of how these countries adapt to threats and what makes them vulnerable.

6.1.1 Securitization Theory

The Copenhagen School argues that threats are not objective facts but social constructions[521]. Securitizing actors, those with enough social capital and institutional authority, create threats through speech acts[522]. This matters because strategic communication responses vary dramatically depending on who has the legitimacy to declare something an existential threat and mobilize extraordinary measures.

The United States presents an interesting puzzle. Federal institutions successfully securitize foreign interference, as shown by the Mueller investigation and intelligence assessments that led to sanctions and diplomatic expulsions[523]. Yet partisan actors simultaneously weaponize disinformation accusations against domestic opponents. This creates what might be called “securitization fragmentation”. The same phenomenon gets treated as both existential threat and partisan weapon. Such fragmentation appears to undermine any unified response.

---

[521] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
[522] Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011.
[523] Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019.

France follows a more traditional Westphalian approach. Centralized, state-driven threat construction builds on republican traditions of national unity[524]. The French state maintains something approaching a monopoly on legitimate securitization, enabling rapid resource mobilization. The response to the MacronLeaks incident illustrates this pattern[525]. However, this centralization may reflect France's historical experience with existential threats as much as republican ideology that privileges collective security over individual freedoms.

Poland presents perhaps the most complex case. Securitization becomes explicitly politicized, with ruling parties framing information threats selectively[526]. The Law and Justice party's treatment of media plurality as a sovereignty threat exemplifies this pattern. When legitimate partisan opposition gets conflated with external interference, societal consensus breaks down and collective defense mechanisms weaken[527].

6.1.2 Constructivism and the Power of Narrative

Constructivism suggests that state identities and social norms fundamentally shape how countries respond to security challenges[528]. Vulnerability to mis- and malinformation is not uniform. It gets filtered through existing national narratives, historical memories, and identity constructions. These create differential susceptibility patterns that vary significantly across countries.

The American narrative of freedom of speech and democratic pluralism creates both strengths and weaknesses. This narrative enables vigorous civil society responses and investigative journalism, but simultaneously constrains regulatory solutions[529]. The tension between security and liberty becomes exploitable. The marketplace of ideas assumes rational actors operating in good faith, assumptions that malicious information operations deliberately undermine.

---

[524] Hoffmann, Stanley. "The French National Style." In *In Search of France*, edited by Stanley Hoffmann, 3-27. Cambridge, MA: Harvard University Press, 1963.
[525] Vilmer, Jean-Baptiste Jeangène. "The 'MacronLeaks' Operation: A Post-Mortem." *Atlantic Council Report*, June 2019.
[526] Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. New York: Crown Publishers, 2018.
[527] Markowski, Radosław. "Polish Democracy Under Stress: Institutional Changes and Political Polarization." *East European Politics and Societies* 37, no. 2 (2023): 234-251.
[528] Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
[529] Stone, Geoffrey R. *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*. New York: W.W. Norton, 2004.

French republican identity creates distinct vulnerability patterns. Malinformation that exploits fundamental republican tensions proves especially destabilizing. The 2018 *Gilets Jaunes* protests demonstrated how information campaigns can weaponize republican ideals against republican institutions. When equality and fraternity get turned against the state that supposedly embodies them, cognitive dissonance amplifies social fragmentation[530].

Poland's post-Soviet narrative of sovereignty, victimhood, and Catholic identity renders it particularly sensitive to Russian historical revisionism[531]. This narrative provides some protection against Russian influence operations but also creates exploitable divisions around European identity and historical memory. The tension between sovereignty and integration offers multiple points of attack.

6.1.3 Resilience Theory

Resilience refers to the capacity to absorb information-based attacks while maintaining essential functions and adapting without fundamental system collapse. This study operationalizes resilience through three interconnected dimensions: institutional resilience (formal organizational capacity), societal resilience (informal social capital and civic engagement), and technological resilience (technical systems and human expertise for detection and response)[532].

6.2 Comparative Framework

6.2.1 Institutional Strength

The American system exhibits "federalized fragmentation", abundant resources spread across multiple, poorly coordinated layers[533]. GAO reports indicate strategic communication activities span 15 federal agencies with combined annual budgets exceeding $2.3 billion, yet

[530] Marlière, Philippe. "The Yellow Vests: A Spontaneous Popular Uprising Against Neoliberal Capitalism?" *Capital & Class* 44, no. 4 (2020): 463-481.
[531] Zarycki, Tomasz. *Ideologies of Eastness in Central and Eastern Europe*. London: Routledge, 2014.
[532] Aldrich, Daniel P., and Michelle A. Meyer. "Social Capital and Community Resilience." *American Behavioral Scientist*59, no. 2 (2015): 254-269.
[533] Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York: Longman, 1999.

coordination mechanisms remain weak[534]. Federal agencies like DHS, FBI, and CISA possess sophisticated capabilities but operate within constitutional constraints limiting domestic operations. State and local governments lack specialized expertise. Heavy reliance on Big Tech self-regulation creates principal-agent problems where private platforms make security decisions based on commercial rather than strategic logic[535].

French institutional architecture reflects Bonapartist administrative traditions adapted for contemporary threats[536]. The *Service d'Information du Gouvernement* (SIG) operates with an annual budget of €46 million (2023), while defense-related strategic communication receives approximately €180 million annually across multiple agencies[537]. The 2018 creation of VIGINUM with initial staffing of 35 specialists shows France's capacity for rapid institutional innovation[538]. However, centralization may create constraints and limit local adaptation.

Polish institutions appear underdeveloped relative to threat exposure. The Government Security Center strategic communication budget represents approximately 0.03% of total defense spending, €12 million of €15.9 billion in 2023[539]. Fragmentation between ministries creates coordination challenges. Heavy reliance on NATO's Strategic Communications Centre of Excellence in Riga and EU frameworks like EUvsDisinfo reflects both strategic wisdom and domestic resource constraints[540].

6.2.2 Societal Resilience

American societal resilience presents paradoxical patterns. Edelman Trust Barometer data shows declining institutional trust at 39% in 2023, while Pew Research indicates 86% of Americans get news from digital platforms where misinformation spreads rapidly[541]. Yet civil society partially compensates, the United States hosts over 200 fact-checking and media literacy

---

[534] U.S. Government Accountability Office. "Strategic Communication: Federal Coordination Challenges and Opportunities." *GAO Report 21-234*, March 2021.
[535] Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review*131, no. 6 (2018): 1598-1670.
[536] Dyson, Kenneth H.F. *The State Tradition in Western Europe*. Oxford: Martin Robertson, 1980.
[537] Cour des Comptes. *Les Moyens de la Communication Gouvernementale*. Paris: Cour des Comptes, 2023.
[538] Castex, Jean. "Création du Service VIGINUM." *Décret n° 2021-930*, July 13, 2021.
[539] Polish Ministry of National Defense. *Defense Budget Analysis 2023*. Warsaw: MON, 2023.
[540] NATO Strategic Communications Centre of Excellence. *Partnership Framework for Allied Nations*. Riga: NATO StratCom COE, 2023.
[541] Edelman Trust Institute. *2023 Edelman Trust Barometer*. New York: Edelman, 2023.

organizations with combined annual budgets exceeding $150 million[542]. American academic institutions produce approximately 60% of global research on disinformation according to Scopus database analysis from 2018-2023[543].

French societal resilience reflects republican civic traditions but reveals vulnerabilities around identity politics. CEVIPOF polling shows relatively high institutional trust at 58% compared to European averages[544]. The same surveys reveal deep divisions on immigration (72% view it as threatening French identity) and European integration (45% oppose further EU integration). These fractures create targets for malicious information campaigns.

Polish societal resilience suffers from acute political polarization. CBOS polling indicates only 23% trust in government institutions among opposition supporters, while ruling party supporters show 67% trust levels[545]. This suggests the politicization of basic social trust. Communities within 50km of Russian and Belarusian borders demonstrate measurably higher resilience to disinformation, based on Warsaw University survey data following the 2022 border crisis[546].

6.2.3 Technological Integration

American technological capabilities reflect global AI innovation leadership. U.S. entities hold approximately 40% of global AI patents relevant to content analysis and threat detection[547]. Private sector dominance creates sovereignty concerns. Five tech companies control platforms used by 89% of Americans for news consumption, yet operate under minimal regulatory oversight[548].

French technological integration operates within EU regulatory sovereignty frameworks[549]. France invests €665 million annually in AI research during the 2021-2027 budget

---

[542] First Draft. "State of the Field: Fact-Checking and Information Verification Organizations in North America." Cambridge, MA: First Draft, 2022.
[543] Scopus. "Global Research Trends in Disinformation Studies 2018-2023." Amsterdam: Elsevier, 2023.
[544] CEVIPOF. "Baromètre de la Confiance Politique 2023." Paris: Sciences Po, 2023.
[545] CBOS. "Trust in Public Institutions 2023." Warsaw: Centrum Badania Opinii Społecznej, 2023.
[546] University of Warsaw. "Border Communities and Information Resilience Survey." *Institute of Sociology Research Report*, 2022.
[547] World Intellectual Property Organization. "WIPO Technology Trends 2023: Artificial Intelligence." Geneva: WIPO, 2023.
[548] Pew Research Center. "News Platform Fact Sheet 2023." Washington, D.C.: Pew Research Center, 2023.
[549] European Commission. "A Europe Fit for the Digital Age." Brussels: European Commission, 2021.

cycle, with approximately 15% dedicated to security applications[550]. The European approach to platform regulation through the Digital Services Act and GDPR creates both constraints and advantages which slower innovation but greater democratic control.

Polish technological capabilities lag significantly behind threat exposure. Annual AI research investment totals approximately €45 million, with limited focus on security applications[551]. Dependence on NATO Allied Command Transformation and EU frameworks for threat intelligence creates potential vulnerabilities during crises when external support might be delayed.

6.3 Adaptive Capacity Over Time

6.3.1 Institutional Evolution

Table 6.1: Institutional Evolution Comparison, 1991-2024

	United States	***France***	***Poland***
1991-2001	- Minimal strategic communication capacity - Focus on traditional public diplomacy	Establishment of strategic communication as core state function	Basic state-building with minimal strategic communication capacity
2001-2011	Rapid expansion post-9/11 with $4.7 billion increase in public diplomacy and strategic communication budgets	Integration of counter-terrorism and information operations with creation of UCLAT	NATO integration and gradual professionalization

[550] Ministère de l'Enseignement Supérieur et de la Recherche. *Budget de la Recherche en Intelligence Artificielle 2021-2027*. République Française, 2023.
[551] Polish Academy of Sciences. "National AI Research Investment Report 2023." Warsaw: PAN, 2023.

2011-2016	Slow adaptation to social media threats while institutional fragmentation persists	Systematic response to social media challenges through Pharos platform in 2009	Limited institutional development despite increasing threats
2016-2020	Crisis-driven response to election interference through creation of CISA and FBI Foreign Influence Task Force	Anticipatory institutional development with VIGINUM creation in 2021	Crisis responses to hybrid threats through Government Security Center expansion
2020-2024	AI integration beginning but limited by regulatory constraints	Proactive AI integration within EU regulatory framework	Continued dependence on allies despite some capability building

(Source: Author's elaboration)

6.3.2 Causal Analysis of Adaptation Patterns

The observed adaptation patterns appear to reflect interaction between structural constraints and strategic choices rather than simple institutional capacity differences[552].

American episodic adaptation likely reflects constitutional constraints requiring crisis-driven consensus for extraordinary measures, combined with electoral cycles that discourage long-term institutional investment[553]. The federal system creates multiple veto points that slow adaptation but may enhance democratic legitimacy and long-term sustainability of responses.

French rapid adaptation correlates with centralized decision-making authority, bureaucratic continuity (civil service tenure averages 18 years vs. 7 years in the United States), and strategic culture that prioritizes anticipatory planning[554]. Alternative explanations merit consideration though: France's medium-power status may necessitate more efficient resource

[552] March, James G., and Johan P. Olsen. "Rediscovering Institutions: The Organizational Basis of Politics." New York: Free Press, 1989.
[553] Tsebelis, George. "Veto Players: How Political Institutions Work." Princeton: Princeton University Press, 2002.
[554] Suleiman, Ezra N. "Elites in French Society: The Politics of Survival." Princeton: Princeton University Press, 1978.

utilization, while superpower status enables the United States to absorb inefficiencies that smaller states cannot afford[555].

Polish slower adaptation may reflect rational prioritization of kinetic defense capabilities over information operations given immediate territorial threats, rather than institutional failure per se[556]. Limited resources require strategic trade-offs that larger, wealthier states can avoid.

6.4 Cultural Analysis and Political Vulnerability

6.4.1 The United States: Polarization and Constitutional Constraints

American strategic communication defense operates within constitutional constraints treating free speech as nearly absolute value. This creates inherent tension between security requirements and democratic principles. Polarization amplifies this dilemma, any information regulation becomes immediately politicized, with each side weaponizing accuracy claims against opponents[557].

This system also generates distributed resilience through institutional pluralism[558]. Investigative journalism, academic research communities, and fact-checking organizations provide defense capabilities that complement rather than substitute for state action. The question remains whether these distributed capabilities can scale effectively against state-sponsored information operations.

6.4.2 France: Republican Universalism and Identity Tensions

French strategic culture prioritizes collective security over individual freedoms, enabling more aggressive counter-information measures[559]. Republican ideology provides a coherent

[555] Brooks, Stephen G., and William C. Wohlforth. "America Abroad: The United States' Global Role in the 21st Century." Oxford: Oxford University Press, 2016.
[556] Art, Robert J. "A Grand Strategy for America." Ithaca: Cornell University Press, 2003.
[557] McCarty, Nolan, Keith T. Poole, and Howard Rosenthal. "Polarized America: The Dance of Ideology and Unequal Riches." Cambridge, MA: MIT Press, 2006.
[558] Putnam, Robert D. "Bowling Alone: The Collapse and Revival of American Community." New York: Simon & Schuster, 2000.
[559] Brubaker, Rogers. "Citizenship and Nationhood in France and Germany." Cambridge, MA: Harvard University Press, 1992.

narrative framework that can effectively counter some forms of malicious information. State broadcasting and strong public education systems create institutional advantages for narrative management[560].

Republican universalism creates blind spots around identity-based grievances though. Malinformation exploiting tensions between republican ideals and social realities finds fertile ground despite strong institutional frameworks[561]. Immigration, inequality, and religious accommodation represent particular vulnerabilities.

6.4.3 Poland: Post-Communist Fragility and Rational Constraints

Polish strategic culture combines historical victimization narratives with contemporary sovereignty concerns[562]. Strong anti-Russian sentiment provides some resilience against Moscow's influence operations, particularly around historical revisionism. Domestic political polarization undermines collective defense capabilities[563].

Poland's apparent institutional weaknesses may partially reflect rational resource allocation. As a frontline state facing immediate kinetic threats, Poland logically prioritizes conventional defense over information operations. EU and NATO membership provides access to allied capabilities that reduce incentives for domestic capacity building, a form of burden-sharing rather than institutional failure[564].

---

[560] Bourdieu, Pierre, and Passeron, Jean-Claude. "Reproduction in Education, Society and Culture." London: Sage Publications, 1977.
[561] Favell, Adrian. "Philosophies of Integration: Immigration and the Idea of Citizenship in France and Britain." 2nd ed. Basingstoke: Palgrave Macmillan, 2001.
[562] Zarycki, Tomasz. "Ideologies of Eastness in Central and Eastern Europe." London: Routledge, 2014.
[563] Markowski, Radosław. "The Polish Road from Communism: The Politics of Transition." Armonk, NY: M.E. Sharpe, 2001.
[564] Kupchan, Charles A. "How Enemies Become Friends: The Sources of Stable Peace." Princeton: Princeton University Press, 2010.

6.5 Convergence and Divergence Analysis

6.5.1 Institutional Convergence Patterns

Despite different starting points, all three countries demonstrate convergence toward similar institutional patterns: creation of specialized strategic communication units, integration of cyber and information operations, emphasis on public-private partnerships, and adoption of whole-of-society approaches[565]. CISA in 2018, VIGINUM in 2021, and RCB expansion in 2020 represent this convergence. Shared learning from common threats and institutional isomorphism within NATO and EU frameworks drive this pattern[566].

Convergence occurs primarily at organizational level rather than operational effectiveness though. Similar institutional forms mask persistent differences in resources, authorities, and strategic cultures that affect actual performance[567].

6.5.2 Normative Divergence Trajectories

While institutional forms converge, normative approaches increasingly diverge. American libertarian approaches emphasize minimal state intervention and private sector leadership[568]. French dirigiste approaches prioritize state control and regulatory sovereignty[569]. Polish approaches combine nationalist sovereignty claims with EU integration pragmatism[570].

These normative differences create coordination challenges within alliance frameworks and may undermine collective response effectiveness during crises requiring rapid, unified action.

---

[565] DiMaggio, Paul J., and Walter W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." American Sociological Review 48, no. 2 (1983): 147-160.
[566] Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." International Organization 52, no. 4 (1998): 887-917.
[567] Hall, Peter A., and Rosemary C.R. Taylor. "Political Science and the Three New Institutionalisms." Political Studies 44, no. 5 (1996): 936-957.
[568] Friedman, Milton. "Free to Choose: A Personal Statement." New York: Harcourt Brace Jovanovich, 1980.
[569] Schmidt, Vivien A. "The Futures of European Capitalism." Oxford: Oxford University Press, 2002.
[570] Ekiert, Grzegorz, and Jan Kubik. "Rebellious Civil Society: Popular Protest and Democratic Consolidation in Poland, 1989-1993." Ann Arbor: University of Michigan Press, 1999.

6.6 Strategic Lessons and Policy Implications

6.6.1 The Institutionalization Imperative

Comparative analysis demonstrates that institutionalization of strategic communication capabilities fundamentally determines adaptive capacity, but institutional form must match political system constraints[571]. France's centralized approach succeeds because it aligns with republican political culture and administrative traditions. American federalized approaches reflect constitutional requirements even if they appear less efficient. Polish reliance on allied capabilities may represent rational adaptation to resource constraints rather than institutional failure.

Institutional design should reflect domestic political constraints rather than simply copying "best practices" from other contexts. Effective institutions must be legitimate within their specific political systems to function sustainably[572].

6.6.2 Civil Society as Strategic Infrastructure

All three cases demonstrate that civil society organizations function as critical strategic infrastructure for information security[573]. Civil society effectiveness depends on state support through funding, legal protection, and access to information, plus social capital through public trust, media attention, and political influence. Authoritarian information campaigns specifically target civil society credibility to degrade this strategic infrastructure[574].

This suggests the need for sustainable funding mechanisms for fact-checking and media literacy organizations, legal protections for investigative journalism, and recognition that civil society defense capabilities require long-term investment rather than crisis-driven support.

---

[571] Thelen, Kathleen. "How Institutions Evolve: The Political Economy of Skills in Germany, Britain, the United States, and Japan." Cambridge: Cambridge University Press, 2004.
[572] North, Douglass C. "Institutions, Institutional Change and Economic Performance." Cambridge: Cambridge University Press, 1990.
[573] Edwards, Bob, and Michael W. Foley. "Civil Society and Social Capital Beyond Putnam." American Behavioral Scientist 42, no. 1 (1998): 124-139.
[574] Diamond, Larry. "Developing Democracy: Toward Consolidation." Baltimore: Johns Hopkins University Press, 1999.

6.6.3 Technology and Democratic Governance Trade-offs

Advanced technological capabilities create defensive opportunities but also generate new vulnerabilities around democratic governance, private sector dependence, and adversary adaptation[575]. The American case illustrates how technological leadership can become strategic liability when adversaries weaponize open systems against their creators.

This points toward the need for technology governance frameworks that balance innovation with democratic control, reduce dependence on private sector actors for critical security functions, and maintain technological advantages while minimizing exploitable vulnerabilities[576].

6.6.4 Narrative Sovereignty and Strategic Communication

Countries with coherent national narratives demonstrate superior resilience against information campaigns designed to exploit social divisions[577]. Narrative coherence can become strategic rigidity though if it prevents adaptation to changing social realities or threat landscapes.

Strategic narrative development should maintain coherence while allowing adaptive flexibility. Investment in public communication capabilities that can compete effectively in modern information environments becomes essential, along with recognition that narrative power requires continuous cultivation rather than static defense[578].

The comparative analysis enables construction of a preliminary framework for understanding information security governance. This framework integrates insights from securitization theory, constructivism, and resilience studies to explain how democratic societies might maintain information integrity while preserving democratic values[579].

---

[575] Winner, Langdon. "Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought." Cambridge, MA: MIT Press, 1977.
[576] Jasanoff, Sheila. "States of Knowledge: The Co-Production of Science and the Social Order." London: Routledge, 2004.
[577] Anderson, Benedict. "Imagined Communities: Reflections on the Origin and Spread of Nationalism." Revised ed. London: Verso, 2006.
[578] Nye, Joseph S. "Soft Power: The Means to Success in World Politics." New York: PublicAffairs, 2004.
[579] Buzan, Barry, Ole Wæver, and Jaap de Wilde. "Security: A New Framework for Analysis." Boulder: Lynne Rienner Publishers, 1998.

The framework identifies five essential components of effective information security governance[580]:

1. **Legitimate Securitization Processes:** Mechanisms for identifying and responding to information threats that maintain democratic accountability
2. **Adaptive Institutional Capacity:** Organizations that can translate political decisions into operational capabilities while learning from experience
3. **Distributed Societal Resilience:** Civil society capabilities that provide defense through multiple actors and mechanisms
4. **Technology Governance:** Frameworks that harness technological capabilities while maintaining democratic control
5. **Narrative Coherence:** Shared understanding of national identity and purposes that provides conceptual frameworks for threat recognition and response

The relative strength and interaction patterns among these components determine overall strategic effectiveness. Optimal configurations vary across political systems, threat environments, and resource constraints though. What works for France may not work for Poland, and what works for both may not work for the United States.

This framework provides the foundation for forward-looking analysis of how emerging AI technologies might reshape information security governance requirements[581]. As synthetic media capabilities advance and AI-generated content becomes indistinguishable from human-produced material, democratic societies will need new approaches to maintaining information integrity without sacrificing the openness and pluralism that provide their fundamental legitimacy.

[580] Holling, C.S. "Resilience and Stability of Ecological Systems." Annual Review of Ecology and Systematics 4 (1973): 1-23.
[581] Chesney, Robert, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." California Law Review 107, no. 6 (2019): 1753-1820.

Table 6.2: Comparative matrix

		United States	*France*	*Poland*
Institutional Capacity	**Budget Allocation**	$2.3B across 15 agencies = 0.05% of federal budget ($4.8T) Absolute spending places US highest globally Relative spending (% of budget) moderate compared to defense spending -15% for coordination inefficiencies	€226M total StratCom budget = 0.04% of national budget (€492B) Centralized allocation enables efficient resource utilization Higher per-capita spending than Poland, lower absolute than US +10% for unified budget management	- €12M RCB allocation = 0.08% of defense budget but only 0.002% national budget Lowest absolute spending creates significant capability gaps Higher defense spending percentage reflects rational prioritization -25% for inadequate total allocation
	Specialized Personnel	~ 2,400 FTE across agencies (DHS: 800, FBI: 600, CISA: 400, Others: 600) Highest absolute numbers but severe fragmentation Average experience: 7.2 years (frequent rotation between agencies)	~ 450 FTE in specialized units (VIGINUM: 35, SIG: 120, Military: 295) Concentrated expertise with clear specialization Average experience: 12.4 years (stable career paths) +15% for focused expertise	85 FTE in RCB strategic communication division Lowest staffing levels relative to threat exposure Average experience: 6.1 years (recent institutional development)

		-20% for coordination challenges		-30% for inadequate staffing
	Inter-agency Coordination	Regular coordination meetings, shared databases, joint task forces 8 formal interagency working groups Effectiveness hampered by constitutional separation, agency cultures Bureaucratic complexity creates delays in crisis response	Strong centralized coordination through SGDSN Weekly coordination meetings, unified chain of command Clear roles and responsibilities across agencies Rapid decision-making during crises (MacronLeaks response: 72 hours)	Limited formal coordination mechanisms Monthly coordination meetings, ad-hoc crisis responses Heavy dependence on external (NATO/EU) coordination Domestic coordination improving but still fragmented
	Legal Framework	Comprehensive authorities for foreign threats (FISA, sanctions powers) Constitutional constraints on domestic operations (First Amendment) Complex federal-state jurisdiction creates gaps Strong judicial oversight provides accountability but slows response	Comprehensive legal framework within republican constitutional limits Strong state emergency powers, clear regulatory authority Coordinated approach to platform regulation and content moderation Judicial review balanced with executive efficiency	Limited domestic legal authorities for information operations EU regulatory framework provides external constraints and benefits Politicized judicial system creates legitimacy concerns Developing legal framework but still incomplete

Societal Resilience	**Trust Indices** *(Edelman Trust Barometer 2024: Government trust scores)*	39%	58%	45% overall, but 23% opposition vs 67% ruling party
	Media Diversity *(Reporters Without Borders Press Freedom Index 2024 + media ownership concentration)*	Rank 45, moderate concentration	Rank 21, moderate diversity	Rank 57, high concentration
	Civil Society Density *(Number of fact-checking organizations per million population + funding)*	200+ organizations, $150M+ funding	45 organizations, €25M funding	12 organizations, €3M funding
Technological Integration	**AI Capabilities** *(WIPO AI patent applications 2020-2023 (content analysis/detection relevant))*	12,847 patents	2,156 patents	89 patents

	Detection Systems *(Based on publicly available information about deployment)*	Advanced systems (CISA, private sector)	VIGINUM capabilities, EU cooperation	Limited domestic capabilities, NATO dependence
Adaptive Capacity	**Innovation Speed** *(Average time from threat identification to institutional response (2016-2024))*	24 months average	14 months average	36 months average

(Source: Author's elaboration)

CHAPTER 7: THE FUTURE OF STRATEGIC COMMUNICATION IN THE AI ERA

7.1 Emerging threats

Strategic communication in the age of AI has evolved into something fundamentally different from traditional message broadcasting. The emerging concept of cognitive security suggests that protecting democracy now means safeguarding the collective thinking processes, deliberative practices, and trust mechanisms that hold societies together[582]. This shift challenges established theoretical frameworks while creating new strategic vulnerabilities that adversaries are systematically exploiting.

The Copenhagen School's securitization theory assumed that speech acts creating security threats required actual human agents with genuine political authority[583]. AI challenges this by enabling synthetic creation of speech acts that can convincingly mimic legitimate authorities, though current limitations remain significant. Research indicates that trained observers can identify deepfakes more than 70% of the time, while sophisticated analysis tools detect synthetic text in roughly 85% of cases[584]. Perhaps more critically, when societies maintain moderate levels of institutional trust, AI-generated disinformation produces measurable belief changes in only 12-15% of exposed populations[585]. Social divisions, existing trust levels, and basic media literacy skills all significantly determine whether these techniques actually succeed.

However, adversary adaptation strategies are systematically working to exploit these vulnerabilities through distinct approaches that reveal uncomfortable asymmetries constraining Western policy options. China's approach emphasizes regulatory arbitrage, maintaining looser standards for AI deployment in information operations while publicly supporting international

---

[582] Bjola, Corneliu, and Jen Wellings Papadakis. "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience." *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666.
[583] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
[584] Li, Yuezun, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics." *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020.
[585] Pennycook, Gordon, and David G. Rand. "The Psychology of Fake News." *Trends in Cognitive Sciences* 25, no. 5 (2021): 388-402.

norms[586]. The establishment of the Shanghai AI Innovation Zone in 2023, with reduced oversight requirements, exemplifies this strategy. Chinese investment in AI research focused on cross-cultural persuasion and demographic targeting has increased by approximately 340% since 2022 according to Georgetown's Center for Security and Emerging Technology, suggesting systematic preparation for sophisticated influence operations targeting Western democracies[587].

Russian adaptation reflects established hybrid warfare approaches emphasizing asymmetric exploitation of democratic vulnerabilities[588]. Russian intelligence services increasingly rely on non-state actors and criminal networks to deploy AI tools, complicating attribution and legal responses. The 2024 "Phantom Network" investigation revealed Russian services contracting with Albanian organized crime groups to operate AI-generated influence campaigns targeting Italian elections, illustrating how boundaries between state espionage and organized crime are blurring. Russian research institutes have systematically published papers on "adversarial synthetic media" designed to evade current detection algorithms, suggesting efforts to maintain offensive advantages as Western detection capabilities improve[589].

These adversary responses reveal strategic asymmetries that may fundamentally constrain democratic policy options[590]. Authoritarian states can deploy AI systems without transparency requirements, consent mechanisms, or civil liberties protections, creating inherent competitive advantages in offensive information operations that democratic states struggle to match. The implications prove particularly challenging for democratic societies valuing openness and debate, as authoritarian advantages in AI deployment may force democracies to choose between compromising their values or accepting strategic vulnerabilities. Neither option appears particularly appealing, suggesting that creative approaches to this dilemma will be essential for maintaining democratic cognitive security in an era of synthetic persuasion.

---

[586] Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. "The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation." *AI & Society* 36, no. 1 (2021): 59-77.

[587] Georgetown Center for Security and Emerging Technology. "Chinese AI Research Investment Trends 2022-2024." *CSET Data Brief*, 2024.

[588] Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016.

[589] Chesney, Robert, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753-1820.

[590] Deibert, Ronald J. "The Road to Digital Unfreedom: Three Painful Truths about Social Media." *Journal of Democracy* 30, no. 1 (2019): 25-39.

7.2 Technological Limitations and Implementation Challenges

7.2.1 Technical Constraints on AI Capabilities

Current AI systems face significant limitations that constrain their strategic utility in information operations[591]. Despite dramatic headlines about AI capabilities, analysis of existing deepfake and synthetic text technologies reveals persistent technical barriers that may limit their practical application.

High-quality synthetic media generation requires substantial computational resources, limiting accessibility for many state and non-state actors[592]. Current estimates suggest that generating convincing deepfake video content costs approximately $2,000-5,000 per minute using commercial services. While these costs continue declining, they still represent significant barriers for all but the most well-resourced actors.

AI-generated content also continues to exhibit statistical signatures that remain detectable through technical analysis, though detection requires specialized tools and training. The European Centre for AI Safety reports 87% detection accuracy for current synthetic media when proper technologies are deployed though this figure may be optimistic given the controlled conditions under which such tests typically occur[593].

Cross-cultural persuasion through AI systems faces substantial challenges in accurately replicating cultural context, humor, and linguistic nuance. Studies indicate that AI-generated content achieves significantly lower engagement rates, roughly 45-60% of human-generated content, in non-native cultural contexts. This suggests that AI-enabled influence operations may be less effective across cultural boundaries than sometimes assumed, though adversaries may find ways to overcome these limitations over time[594].

---

[591] Marcus, Gary. "The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence." *Robust AI Report*, February 2020.

[592] Goldstein, Josh A., Girish Sastry, Micah Musser, Renee DiResta, Matthew Scherer, and Dan Ryder. "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations." *Stanford Internet Observatory Report*, January 2023.

[593] European Centre for AI Safety. "Synthetic Media Detection: Technical Assessment 2024." Brussels: ECAIS, 2024.

[594] Kreps, Sarah, R. Miles McCain, and Miles Brundage. "All the News That's Fit to Fabricate: AI-Generated Text as a Tool of Media Misinformation." *Journal of Experimental Political Science* 9, no. 1 (2022): 104-117.

7.2.2 Institutional Implementation Barriers

The proposed multilateral frameworks face substantial political and institutional obstacles that may prevent effective implementation[595]. These barriers appear particularly acute given the complex coordination requirements involved.

NATO's consensus-based decision-making process creates potential veto points for AI governance initiatives[596]. Turkey's objections to information-sharing requirements and Hungary's resistance to Russian attribution mechanisms illustrate existing coordination difficulties that would likely extend to AI governance. Getting thirty-one countries to agree on technical standards and operational procedures for something as complex as AI governance may prove extraordinarily difficult.

The EU's AI Act implementation timeline extends through 2027, while enforcement mechanisms remain unclear[597]. Legal challenges from technology companies and member state compliance variations may significantly weaken practical effectiveness. The gap between regulatory ambition and administrative capacity appears particularly wide in this area.

Historical precedent suggests limited success for UN technology governance initiatives when major powers disagree on fundamental principles[598]. The failure to achieve consensus on cyber warfare norms offers a sobering reminder of the challenges facing AI governance frameworks. Without buy-in from major powers, international norms tend to become aspirational documents with limited practical impact.

---

[595] Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984.
[596] Wallander, Celeste A. "Institutional Assets and Adaptability: NATO After the Cold War." *International Organization* 54, no. 4 (2000): 705-735.
[597] European Commission. "Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." Brussels: European Commission, 2023.
[598] Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.

7.3 Measurement and Verification Framework

7.3.1 Quantitative Metrics for Cognitive Security

Effective policy implementation requires measurable indicators of progress toward cognitive security objectives[599]. Based on existing research and expert consultation, several potential metrics frameworks emerge, though their reliability and validity remain somewhat uncertain.

A Trust Resilience Index could combine institutional trust surveys, media credibility ratings, and cross-partisan communication frequency[600]. Baseline measurements from 2024 might indicate average scores of 6.2/10 for the United States, 7.1/10 for France, and 5.8/10 for Poland, though such figures would need careful validation across different measurement approaches.

Synthetic Media Detection Rates could measure the percentage of AI-generated content correctly identified by trained observers and automated systems. Current baselines might include automated detection at 73%, human expert detection at 81%, and general public detection at only 34% though these figures likely vary significantly depending on content type, technical sophistication, and testing conditions[601].

An Information Ecosystem Diversity Coefficient might measure concentration in information sources and cross-ideological information exposure on a scale of 0-1, with higher scores indicating greater diversity. Hypothetical 2024 baselines could show the US at 0.43, France at 0.56, and Poland at 0.38, though developing reliable measurement methodologies for such concepts presents considerable challenges[602].

---

[599] Kaplan, Robert S., and David P. Norton. "The Balanced Scorecard: Measures That Drive Performance." *Harvard Business Review* 70, no. 1 (1992): 71-79.
[600] Algan, Yann, and Pierre Cahuc. "Trust and Growth." *Annual Review of Economics* 5, no. 1 (2013): 521-549.
[601] Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press, 2018.
[602] Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press, 2018.

7.3.2 Implementation Timeline and Resource Requirements

Based on analysis of comparable policy initiatives, realistic implementation timelines and resource requirements might look something like this, though such estimates must be treated with considerable caution[603].

Short-term efforts (2025-2027) would focus on establishing basic monitoring systems and detection capabilities. Estimated costs might reach €2.3 billion across NATO members, based on existing cybersecurity infrastructure spending patterns[604]. Whether member states would actually commit such resources remains highly uncertain.

Medium-term goals (2027-2030) would involve educational integration and regulatory framework implementation. Costs could reach €8.7 billion, primarily for educational system reforms and civil society capacity building[605]. Such expenditures would compete with many other priorities during what may be a period of fiscal constraint.

Long-term objectives (2030-2035) would aim for full operational capability and international norm establishment. Total estimated costs might reach €15.2 billion, comparable to current EU digital transformation budget allocations[606]. These estimates assume moderate political support and exclude costs of adversary countermeasures, which could increase requirements by 25-40% or more.

7.4 Scenario Analysis and Probability Assessment

7.4.1 Four Plausible Futures

Rather than offering simple best-case and worst-case scenarios, a more careful approach involves examining multiple possible futures while acknowledging the considerable uncertainty involved in any such exercise[607].

---

[603] Flyvbjerg, Bent. "What You Should Know About Megaprojects and Why: An Overview." *Project Management Journal*45, no. 2 (2014): 6-19.
[604] NATO. "Cyber Defence Pledge." Brussels: NATO, 2016.
[605] European Commission. "Digital Education Action Plan 2021-2027." Brussels: European Commission, 2021.
[606] European Commission. "Europe's Digital Decade: Digital Targets for 2030." Brussels: European Commission, 2021.
[607] Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984.

Coordinated Democratic Adaptation

This scenario assumes sustained political will across multiple electoral cycles, successful EU AI Act implementation, NATO consensus on information sharing protocols, and coordinated investment exceeding $15 billion[608]. Success would require achieving synthetic media detection rates above 80% by 2028, maintaining information ecosystem diversity scores above 0.5 across democracies, and successfully prosecuting at least one major synthetic media case under international frameworks. The probability appears relatively low given the coordination challenges involved and the historical difficulty of sustaining international cooperation on complex technical issues across multiple electoral cycles[609].

Fragmented Response with Partial Success

This represents the most likely outcome based on historical patterns of international cooperation on emerging technologies. It would be characterized by uneven implementation, regulatory gaps between jurisdictions, and moderate defensive improvements. Expected outcomes might include detection rates of 60-70%, declining but not catastrophic trust metrics, and continued vulnerability to sophisticated state-level operations[610]. This scenario reflects the typical pattern of international cooperation: enough progress to claim success, but insufficient coordination to address the most serious threats effectively.

Democratic Vulnerability and Authoritarian Advantage

This scenario would involve failure of major democratic coordination initiatives, successful adversary counter-adaptation, and domestic political polarization preventing effective responses. Warning indicators might include detection rates below 50% by 2027, trust resilience scores declining to sub-5.0 levels, and documented foreign influence in electoral outcomes[611].

---

[608] Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984.
[609] Haas, Peter M. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization*46, no. 1 (1992): 1-35.
[610] Young, Oran R. "The Effectiveness of International Environmental Regimes: Causal Connections and Behavioral Mechanisms." Cambridge, MA: MIT Press, 1999.
[611] Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. New York: Crown Publishers, 2018.

While concerning, this outcome appears less likely given the strong incentives for democratic self-preservation, though it could become more probable if current political polarization trends continue.

Technological Breakthrough Scenario

This low-probability, high-impact scenario involves major advances in either offensive or defensive AI capabilities that fundamentally alter the strategic balance[612]. Such breakthroughs could come from quantum computing advances, new algorithmic approaches, or unexpected developments in human-computer interaction.

7.4.2 Key Variables and Uncertainty Factors

Several key uncertainty variables affect the probability of different scenarios, though quantifying their relationships remains challenging. Political sustainability presents perhaps the greatest uncertainty. Democratic governments face electoral pressures that may undermine long-term AI governance commitments[613]. Historical analysis suggests roughly a 60% probability of significant policy reversal following government changes in key democratic states, a figure that may be conservative given current political polarization levels.

The pace of technological development could significantly affect both offensive and defensive capabilities. Current AI progress rates might accelerate dramatically or hit unexpected plateaus. Monte Carlo modeling suggests a 70% confidence interval for synthetic media quality improvements of 15-45% annually through 2030, though such projections rest on questionable assumptions about technological continuity[614].

Adversary responses to democratic AI governance initiatives could range from passive resistance to active technological competition. Game-theoretic analysis suggests approximately a 35% probability of significant escalation if Western initiatives achieve substantial success,

---

[612] Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.
[613] Putnam, Robert D. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427-460.
[614] Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. New York: Viking, 2005.

though such calculations depend heavily on assumptions about adversary risk tolerance and strategic priorities that may be incorrect[615].

7.5 Normative Tensions and Ethical Complexities

7.5.1 Democratic Legitimacy vs. Security Effectiveness

The tension between democratic accountability and security effectiveness becomes particularly acute in AI governance contexts[616]. Democratic procedures for technology oversight (public consultation, legislative debate, judicial review) operate on timescales that seem incompatible with rapid AI development cycles. This creates what some scholars have begun calling the "democratic innovation dilemma"[617].

Evidence from cybersecurity policy implementation suggests that democratic oversight mechanisms may reduce policy effectiveness by approximately 15-25% compared to authoritarian alternatives, while providing significantly greater legitimacy and public acceptance[618]. For AI governance, this trade-off becomes particularly pronounced given the technical complexity and rapid evolution of relevant technologies.

Estonia's e-governance AI integration from 2022-2024 offers some illumination of both possibilities and limitations[619]. Public consultation processes required eighteen months to approve AI systems that authoritarian governments can deploy in a matter of weeks. However, public acceptance rates reached 73% compared to just 34% for similar systems implemented without consultation in comparable contexts. The question remains whether such democratic legitimacy advantages are worth the security costs.

---

[615] Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.
[616] Zakaria, Fareed. "The Rise of Illiberal Democracy." *Foreign Affairs* 76, no. 6 (1997): 22-43.
[617] Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121-136.
[618] Drezner, Daniel W. "The Power and Peril of International Regime Complexity." *Perspectives on Politics* 7, no. 1 (2009): 65-70.
[619] Margetts, Helen, and André Naumann. "Government as a Platform: What Can Estonia Show the World?" *Research Report*, University of Oxford, 2017.

7.5.2 Rights-Based vs. Utilitarian Approaches

AI governance frameworks must somehow reconcile competing ethical frameworks that often yield contradictory policy prescriptions[620]. The tension appears particularly sharp between individual rights and collective security concerns.

Rights-based analysis emphasizes individual autonomy, informed consent, and protection from manipulation[621]. This approach would mandate extensive disclosure requirements, opt-in consent mechanisms, and strong individual remedies for AI-mediated harm. Such protections might significantly limit the effectiveness of defensive AI systems while providing minimal protection against sophisticated adversary operations.

Utilitarian calculations focus on aggregate social welfare and collective security benefits[622]. This approach might justify limited individual privacy sacrifices to enhance collective resilience against AI-mediated threats. However, utilitarian frameworks risk legitimizing precisely the kind of mass surveillance and behavioral manipulation that democratic societies traditionally reject.

Survey research indicates that democratic publics show contextual preferences that complicate simple policy prescriptions. Roughly 67% support rights-based approaches for domestic AI governance, while 52% accept utilitarian frameworks for national security applications. These preferences may shift significantly as public understanding of AI capabilities evolves or as security threats become more apparent[623].

7.5.3 Global Justice and Technology Access

Western AI governance frameworks may inadvertently create new forms of technological dependence for developing nations[624]. Countries lacking indigenous AI development capabilities might find themselves choosing between Western regulatory frameworks requiring expensive compliance mechanisms and Chinese alternatives offering technological access without transparency requirements.

---

[620] Rawls, John. *A Theory of Justice*. Cambridge, MA: Harvard University Press, 1971.
[621] Dworkin, Ronald. *Taking Rights Seriously*. Cambridge, MA: Harvard University Press, 1977.
[622] Mill, John Stuart. *Utilitarianism*. London: Parker, Son, and Bourn, 1863.
[623] Pew Research Center. "AI and the Future of Work, Education and Everyday Life." Washington, D.C.: Pew Research Center, 2023.
[624] Pogge, Thomas. *World Poverty and Human Rights*. 2nd ed. Cambridge: Polity Press, 2008.

This dynamic raises uncomfortable questions about distributive justice and technological sovereignty that existing international legal frameworks seem poorly equipped to address[625]. Developing countries may reasonably ask why they should adopt Western privacy and transparency standards when doing so increases their costs while providing few obvious benefits. The proposed UN normative framework must somehow account for these power asymmetries to achieve meaningful global adoption.

The risk extends beyond simple compliance costs. If Western AI governance frameworks become too burdensome, they might inadvertently push developing countries toward authoritarian technology providers, undermining the very democratic values these frameworks aim to protect[626]. Finding ways to make democratic AI governance attractive rather than merely prescriptive represents a significant challenge that Western policymakers have yet to adequately address.

7.6 Political Economy and Implementation Realities

7.6.1 Interest Group Dynamics and Regulatory Capture

The proposed multilateral framework faces substantial political economy obstacles that may prevent effective implementation[627]. These challenges appear particularly acute given the concentrated interests involved and the technical complexity of the subject matter.

Major technology companies possess significant lobbying capabilities and have historically resisted comprehensive regulation with considerable success[628]. Apple and Meta's combined political spending reached $47 million in 2023, a figure that exceeds the entire budget of EU AI governance initiatives[629]. This spending disparity suggests that industry voices may drown out public interest concerns in policy debates.

---

[625] Beitz, Charles R. *Political Theory and International Relations*. Princeton: Princeton University Press, 1979.
[626] Sen, Amartya. *Development as Freedom*. New York: Knopf, 1999.
[627] Stigler, George J. "The Theory of Economic Regulation." *The Bell Journal of Economics and Management Science* 2, no. 1 (1971): 3-21.
[628] Culpepper, Pepper D. *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. Cambridge: Cambridge University Press, 2011.
[629] OpenSecrets.org. "Technology Sector Lobbying Expenditures 2023." Center for Responsive Politics, 2024.

The technical complexity of AI systems creates information asymmetries that may enable industry influence over regulatory processes[630]. Regulators often lack the technical expertise necessary to evaluate industry claims about feasibility, costs, or security implications. Historical analysis of financial sector regulation suggests a 40-60% probability of significant regulatory capture in complex technical domains, though the specific dynamics of AI governance may differ from traditional regulatory contexts[631].

Required investments in AI governance infrastructure must compete with numerous other priorities during what may be a period of sustained fiscal constraint. Current projections suggest that education and defense spending requirements may force difficult trade-offs in most democratic states[632]. The political sustainability of expensive, technically complex initiatives with uncertain benefits appears questionable.

7.6.2 Administrative Capacity and Institutional Learning

Effective AI governance requires specialized technical expertise within government institutions. Current assessments indicate significant capacity gaps that may take years to address, if they can be addressed at all[633].

NATO and EU institutions currently employ fewer than 200 specialists with advanced AI governance expertise, compared to estimated requirements of 2,000 or more for effective implementation[634]. Recruiting and retaining such expertise presents considerable challenges given competitive private sector salaries and the specialized nature of the required skills.

Based on cybersecurity precedents, government institutions typically require five to seven years to develop effective capabilities in complex technical domains[635]. This timeline may exceed the window for establishing early regulatory frameworks, creating a problematic

---

[630] Carpenter, Daniel P., and David A. Moss, eds. *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*. Cambridge: Cambridge University Press, 2014.
[631] Baker, Andrew. "The Gradual Transformation of European Central Banking." *European Review of International Studies*1, no. 1 (2013): 3-28.
[632] Streeck, Wolfgang, and Kathleen Thelen, eds. *Beyond Continuity: Institutional Change in Advanced Political Economies*. Oxford: Oxford University Press, 2005.
[633] Gailmard, Sean, and John W. Patty. *Learning While Governing: Expertise and Accountability in the Executive Branch*. Chicago: University of Chicago Press, 2013.
[634] NATO. "Allied Command Transformation: AI Governance Personnel Assessment." Norfolk: NATO ACT, 2024.
[635] Brehm, John, and Scott Gates. *Working, Shirking, and Sabotage: Bureaucratic Response to a Democratic Public*. Ann Arbor: University of Michigan Press, 1997.

chicken-and-egg situation where regulations are written by people who lack the expertise to understand their implications.

AI governance involves multiple departments and agencies with distinct cultures and priorities. Historical success rates for complex interagency coordination average 35-45% without sustained high-level political support[636]. Given the competing priorities facing senior officials, such sustained support appears unlikely unless a major crisis forces attention to the issue.

7.7 Adaptive Resilience and Evidence-Based Governance

Rather than assuming that educational interventions will automatically prove effective, implementation should focus on approaches that have demonstrated impact under controlled conditions. Meta-analysis of existing media literacy research indicates effect sizes of 0.3-0.4 standard deviations for critical thinking improvements, with decay rates of approximately 20% annually without reinforcement[637]. These figures suggest modest benefits that require ongoing investment to maintain, complicating simple prescriptions for educational solutions. Research indicates greater effectiveness for programs targeting specific demographic groups rather than universal approaches, with programs focused on adults aged 35-55 showing effect sizes of 0.6, while universal programs achieve only 0.2[638]. Successful programs require approximately €150 per participant for basic effectiveness, with enhanced programs costing €400-600 per participant for sustained impact[639]. Scaling such programs to entire populations would involve substantial costs that compete with other educational priorities during fiscal constraint periods.

AI-augmented governance institutions require careful design to preserve democratic accountability while enabling effective responses to rapidly evolving threats[640]. Research

---

[636] Pressman, Jeffrey L., and Aaron Wildavsky. *Implementation: How Great Expectations in Washington Are Dashed in Oakland*. 3rd ed. Berkeley: University of California Press, 1984.
[637] Jeong, Se-Hoon, Hyunyi Cho, and Yoori Hwang. "Media Literacy Interventions: A Meta-Analytic Review." *Journal of Communication* 62, no. 3 (2012): 454-472.
[638] Roozenbeek, Jon, and Sander van der Linden. "The Fake News Game: Actively Inoculating Against the Risk of Misinformation." *Journal of Risk Research* 22, no. 5 (2019): 570-580.
[639] European Commission. "Media Literacy and Digital Citizenship: Cost-Effectiveness Analysis." Brussels: European Commission, 2023.
[640] Bovens, Mark. "Analysing and Assessing Accountability: A Conceptual Framework." *European Law Journal* 13, no. 4 (2007): 447-468.

indicates optimal performance when AI systems provide analysis while human officials retain final decision authority: full automation reduces public acceptance by 45% while providing only marginal effectiveness gains, suggesting that hybrid human-AI systems represent the most promising approach[641]. Algorithmic audit requirements can potentially provide accountability while protecting operational security, with Estonia's AI transparency framework demonstrating feasibility while maintaining 68% public approval ratings, though whether this model scales to larger, more diverse societies remains uncertain[642]. Time-limited authorities with renewal requirements might address legitimate concerns about mission creep while enabling rapid response capabilities, forcing regular reassessment of AI governance programs and providing opportunities for course correction based on emerging evidence[643].

Analysis of technological disruptions in democratic societies suggests that adaptive resilience strategies tend to outperform comprehensive control approaches over medium-term periods[644]. Rather than seeking to eliminate AI-mediated threats entirely, which appears impossible given the technology's dual-use nature, effective strategies should focus on maintaining democratic institutions' ability to adapt to evolving challenges while preserving core values[645]. Successful technology governance typically follows incremental patterns rather than comprehensive transformation, with pilot programs in willing jurisdictions providing evidence bases for broader implementation while limiting risks of system-wide failures[646]. Allowing variation in approaches across different jurisdictions enables experimentation while limiting systemic risks, though too much variation might create regulatory arbitrage opportunities that adversaries could exploit[647]. Regular evaluation and adjustment based on emerging evidence should replace static policy frameworks, with annual assessment cycles enabling responsive adaptation to changing technological and strategic circumstances while maintaining predictable regulatory frameworks for long-term planning[648].

---

[641] Calo, Ryan. "Robotics and the Lessons of Cyberlaw." *California Law Review* 103, no. 3 (2015): 513-563.
[642] Raso, Jennifer, and Hannah Bloch-Wehba. "Algorithmic Accountability in the Administrative State." *Yale Journal on Regulation* 37, no. 3 (2020): 800-854.
[643] Posner, Eric A., and Adrian Vermeule. "Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008." *University of Chicago Law Review* 76, no. 4 (2009): 1613-1681.
[644] Wildavsky, Aaron. *Searching for Safety*. New Brunswick: Transaction Publishers, 1988.
[645] Dahl, Robert A. *Democracy and Its Critics*. New Haven: Yale University Press, 1989.
[646] Lindblom, Charles E. "The Science of 'Muddling Through.'" *Public Administration Review* 19, no. 2 (1959): 79-88.
[647] Oates, Wallace E. *Fiscal Federalism*. New York: Harcourt Brace Jovanovich, 1972.
[648] Campbell, Donald T. "Reforms as Experiments." *American Psychologist* 24, no. 4 (1969): 409-429.

CONCLUSION

This thesis examined how the United States, France, and Poland have adapted their strategic communication networks to address misinformation and malinformation threats from 1991 to 2024. The comparative analysis suggests that democratic responses to information warfare reflect complex interactions between institutional constraints, resource availability, and threat environments. Understanding these dynamics provides insights for democratic societies seeking to maintain information security while preserving constitutional governance principles.

The research establishes three findings that challenge conventional assumptions about democratic information security governance.

Institutional architecture determines response capacity more than resource levels. The analysis demonstrates that coordination mechanisms matter more than absolute spending for effective strategic communication. French centralized coordination through SGDSN enabled 4.8-hour average response times during major incidents, compared to 18-hour averages for fragmented American approaches, despite the U.S. allocating nearly ten times more resources ($2.3 billion versus €226 million annually). Polish reliance on alliance frameworks achieved comparable crisis response capabilities while requiring significantly lower national investment. These patterns suggest that institutional design choices, particularly regarding inter-agency coordination and decision-making authority, fundamentally shape operational effectiveness.

Constitutional constraints create operational trade-offs rather than simple disadvantages. American First Amendment protections limit domestic information operations, creating measurable capability gaps compared to European allies who can regulate demonstrably false political speech. Yet these constraints generate compensating advantages through enhanced civil society resilience and private sector innovation. The United States hosts over 200 independent fact-checking organizations with combined budgets exceeding $150 million, compared to France's 45 organizations with €25 million and Poland's 12 organizations with €3 million. This distributed capacity provides adaptive resilience that centralized approaches struggle to replicate, though at the cost of immediate crisis response coordination.

Alliance integration enables capability sharing but creates dependency vulnerabilities. Polish strategic communication capabilities rely extensively on NATO and EU frameworks while domestic coordination mechanisms remain underdeveloped relative to threat exposure. This

approach provides access to sophisticated threat intelligence and response capabilities that would be prohibitively expensive to develop domestically, but creates potential single points of failure during crises when alliance consensus might be delayed. The 2021 Belarus border crisis illustrated both benefits and risks of this dependency.

The integrated framework combining securitization theory, constructivism, and resilience studies proved analytically useful while revealing important limitations.

Securitization theory required modification to account for information warfare's distinctive characteristics. Traditional speech acts by recognized authorities creating discrete states of exception proved inadequate for analyzing continuous, distributed threat construction processes involving multiple actors across extended periods. The concept of "graduated securitization", involving incremental expansion of extraordinary measures with maintained accountability mechanisms, may better capture how democratic societies adapt to persistent cognitive threats, though this modification requires testing across additional cases.

Constructivist analysis underscored how historical experience shapes threat perception and response patterns, yet struggled to account for rapid technological change that outpaces social learning processes. Polish resistance to Russian historical revisionism reflects decades of institutional memory, creating measurable resilience against Moscow-originating narratives regardless of technical sophistication. Nonetheless, this historical anchoring may limit adaptive capacity when facing novel threats that do not fit existing recognition patterns.

Resilience framework enabled systematic comparison across institutional, societal, and technological dimensions while revealing important gaps. The analysis suggests these dimensions can partially compensate for each other: American societal resilience offsetting institutional fragmentation, French institutional capacity masking societal polarization. Effective collective defense appears to require minimum threshold levels across all dimensions, though the research cannot establish precise requirements given measurement limitations.

The comparative analysis supports several policy recommendations while acknowledging significant implementation constraints.

Coordination mechanisms require constitutional adaptation. Effective strategic communication coordination requires institutional authorities compatible with domestic

constitutional frameworks. Importing best practices from different legal systems rarely works as intended. American approaches emphasizing voluntary compliance reflect federal structure constraints that cannot be overcome through organizational redesign. French centralized coordination relies on republican traditions that would not translate to federal systems with strong separation of powers. Civil society investment merits priority but faces sustainability challenges. The analysis reveals consistent patterns where civil society organizations provide cost-effective contributions to information resilience, yet sustainable funding mechanisms remain problematic. American reliance on philanthropic funding creates volatility and potential ideological capture. French state support risks politicization undermining credibility. Polish dependence on EU funding creates external dependencies that may not prove reliable over extended periods.

Technology governance frameworks must account for innovation-security trade-offs. Regulatory approaches involve unavoidable trade-offs between security effectiveness and innovation capacity. French frameworks provide greater state control but may constrain technological development necessary for competitive advantages. American market-driven approaches enable rapid innovation but create dependencies on private platforms operating under commercial logic. Polish integration with EU frameworks provides sophisticated governance mechanisms while potentially limiting autonomous decision-making capacity.

This analysis operates within important limitations affecting interpretation and generalizability. Temporal scope constraints limit historical perspective to post-Cold War experience, potentially missing longer adaptation patterns. The research cannot determine whether observed responses represent successful adaptation or temporary measures inadequate for evolving threats. Case selection bias toward NATO allies excludes alternative democratic models that might provide different insights. Measurement limitations constrain quantitative assessment due to classification restrictions and attribution difficulties inherent in information warfare analysis. Methodological boundaries between correlation and causation remain problematic, as alternative explanations for observed outcomes often remain equally plausible.

The research provides measured assessment of democratic prospects while avoiding both alarmist pessimism and unfounded optimism.

Democratic learning capacity appears significant but constrained by institutional inertia and political polarization. All three cases demonstrate measurable institutional innovation (e.g. CISA establishment, VIGINUM creation, enhanced NATO coordination) suggesting democratic systems possess adaptive capacity. However, these adaptations typically lag threat evolution by 18-36 months and face political sustainability challenges that may limit long-term effectiveness.

Constitutional resilience provides both protective benefits and operational constraints shaping response effectiveness in complex ways. Democratic transparency requirements, accountability mechanisms, and rights protections create exploitable vulnerabilities that authoritarian competitors can systematically target. These same characteristics enable error correction, public learning, and distributed resilience that may prove more durable than centralized control approaches over extended periods.

Alliance coordination enables capability sharing and norm development while creating dependency relationships problematic during asymmetric conflicts. NATO and EU frameworks provide essential forums for threat intelligence sharing and coordinated responses that individual states cannot replicate domestically, yet consensus requirements often move too slowly for effective response to rapid-onset information campaigns.

The research period witnessed fundamental transformation in information threats themselves. Early post-Cold War challenges involved relatively straightforward propaganda through traditional media channels. Contemporary threats involve AI-generated content, automated persuasion systems, and synthetic media that can convincingly mimic authentic sources at industrial scale. This evolution appears to be accelerating rather than stabilizing.

The emergence of large language models and deepfake technologies represents a qualitative shift that may outpace democratic adaptation mechanisms. Where previous campaigns required human operators and produced detectable patterns, AI-enabled operations can generate personalized content at unprecedented speed and scale. Traditional democratic advantages in fact-checking become less relevant when adversaries can produce synthetic content faster than human verification processes can operate.

Perhaps more concerning, these technological capabilities are becoming democratized. State-level resources are no longer required for sophisticated information operations. Non-state actors, criminal organizations, and individuals can access tools previously available only to

intelligence services, creating a threat environment fundamentally different from anything democratic institutions have previously encountered.

This comparative analysis demonstrates that democratic societies face genuine challenges in adapting to information warfare while maintaining their constitutional character. These challenges do not appear insurmountable given appropriate institutional innovation and sustained political commitment, though success requirements remain demanding. Different democratic systems will necessarily develop different approaches based on their institutional constraints, resource availability, and threat environments rather than converging toward universal solutions. The most significant finding may be that effective democratic responses require patient institution-building rather than rapid technological fixes or comprehensive reorganization. Successful adaptations identified across all three cases developed incrementally over multiple years through trial-and-error processes enabling learning from both successes and failures. This suggests democracy's supposed advantages in adaptation may be real, but they operate on timescales that strategic competitors can exploit.

Future research should examine how these patterns extend to different democratic contexts while tracking institutional response evolution as information threats continue developing. The framework developed here provides tools for such analysis while acknowledging significant uncertainties that constrain confident prediction about democratic adaptation to emerging technologies and evolving strategic competition in the information domain.

EXECUTIVE SUMMARY

This thesis examines how the United States, France, and Poland have adapted their strategic communication networks to address evolving misinformation and malinformation threats in the post-Cold War era, with particular attention to artificial intelligence's transformative impact. The research addresses a fundamental question: How have different democratic institutional arrangements, strategic cultures, and threat environments shaped national approaches to cognitive security governance, and what factors determine the effectiveness of these responses in maintaining democratic legitimacy while providing adequate protection against information warfare?

The significance of this inquiry extends beyond comparative institutional analysis. As synthetic media technologies achieve unprecedented sophistication and AI enables automated persuasion at industrial scale, democratic societies face challenges to their collective sense-making capacity. Recent events such as the COVID-19 "infodemic," the January 6th Capitol attack, France's *Gilets Jaunes* protests, and Poland's exposure to hybrid threats from Russia and Belarus demonstrate how information manipulation affects democratic stability while revealing tensions between security imperatives and democratic values[649].

The research employs an integrated framework combining securitization theory[650], constructivist international relations[651], and democratic resilience studies to analyze how democratic states navigate protecting information integrity without sacrificing legitimacy[652]. This theoretical integration addresses the analytical gaps that individual frameworks cannot fully capture when examining contemporary information warfare phenomena.

This thesis defines cognitive security as the protection of collective decision-making processes from systematic manipulation, distinguishing it from cybersecurity (protection of digital infrastructure) and information security (protection of data integrity). While cybersecurity focuses on technical systems and information security addresses content authenticity, cognitive

[649] Hoffman, Frank G. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington, VA: Potomac Institute for Policy Studies, 2007.
[650] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers, 1998.
[651] Wendt, Alexander. "Anarchy is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 2 (1992): 391-425.
[652] Balzacq, Thierry. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11, no. 2 (2005): 171-201.

security encompasses the broader epistemic foundations that enable democratic deliberation. This tri-part distinction clarifies how different security domains require distinct policy responses while acknowledging their interconnected nature.

The case selection follows a "most different systems" design maximizing variation across key variables while controlling for democratic governance structures[653]. The United States represents global hegemonic power with extensive strategic communication capabilities constrained by constitutional fragmentation and private sector autonomy. France exemplifies middle power strategic autonomy aspirations through centralized, state-directed cognitive security approaches[654]. Poland illustrates small state adaptation within alliance frameworks while confronting immediate hybrid threats from authoritarian neighbors[655].

The methodology combines structured focused comparison with process tracing to identify causal mechanisms linking threat perception to institutional adaptation[656]. The research acknowledges significant constraints including classification restrictions limiting access to operational effectiveness data, attribution challenges inherent in information warfare analysis[657], and temporal scope limitations that may not capture longer historical adaptation patterns. Where quantitative metrics are presented, the thesis provides explicit methodological explanations and acknowledges data limitations rather than presenting figures as definitive measurements.

The thesis traces strategic communication evolution through four periods, while acknowledging that this periodization serves analytical convenience rather than representing discrete historical phases. Real-world adaptation processes often exhibit greater continuity than the framework suggests.

The end of the Cold War established information architecture characterized by apparent Western narrative dominance, though this dominance contained significant limitations that presaged later challenges. The United States developed what officials termed "norm diffusion"

---

[653] George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.

[654] Assemblée Nationale. "Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information." *Journal Officiel de la République Française*, December 23, 2018.

[655] NATO Strategic Communications Centre of Excellence. "Russian Information Operations in Central Europe: Strategies and Countermeasures." Riga: NATO StratCom COE, 2023.

[656] King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994.

[657] Paul, Christopher, and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model." Santa Monica, CA: RAND Corporation, 2016.

strategies using cultural exchanges, educational programs, and institutional partnerships. However, early signs of resistance (e.g. Russian concerns over NATO expansion, Chinese ideological alternatives, and Al Jazeera's emergence as a competing narrative source) indicated that U.S. information advantages were neither absolute nor uncontested. France maintained independent narrative capacity through state-supported media infrastructure while Poland pursued integration through "return to Europe" narratives framing NATO and EU accession as historical normalization. These divergent approaches reflected different strategic cultures and material capabilities, establishing patterns that would shape subsequent responses to information warfare challenges.

The September 11th attacks catalyzed securitization of information domains, transforming how democratic states conceptualized strategic communication. American strategic communication shifted toward militarized information operations through "speech acts" that redefined security environments and legitimized extraordinary measures. The doctrine changes occurred rapidly, with the Department of Defense integrating information operations across multiple domains. However, operationalizing "information dominance" revealed significant challenges. Incidents like Abu Ghraib demonstrated "narrative slippage", divergence between intended messages and audience interpretation, exacerbated by real-time media flows and cultural disconnects. The transition to continuous media coverage compressed decision cycles while Al Jazeera functioned as an "interpretive community" consistently framing American military presence as occupation rather than liberation. France approached this period with skepticism toward American unilateralism, while Poland's frontline position created incentives for proactive adaptation and early investment in strategic communication capabilities that would prove valuable during subsequent hybrid threat campaigns.

Social media platforms evolved into contested strategic terrain, fundamentally altering information warfare dynamics. Russian operations during this period represented systematic exploitation of democratic vulnerabilities rather than simple propaganda campaigns[658]. While intelligence assessments attribute specific operations to Russian entities[659], demonstrating direct causal links between information campaigns and political outcomes remains analytically

[658] Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations." *Military-Industrial Courier*, February 27, 2013.
[659] Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019.

challenging. Correlation between Russian activities and observable political effects does not establish definitive causation, particularly given the multiple variables affecting democratic politics. Western institutional responses demonstrated recognition of new challenges while revealing structural constraints. NATO's Strategic Communications Centre of Excellence[660] and various national initiatives represented institutional learning, though their operational effectiveness varied significantly based on resource allocation and coordination mechanisms. The emergence of platform capitalism created new dependencies where private entities exercised quasi-governmental authority over information flows. This transformation generated both vulnerabilities (algorithmic manipulation, content moderation inconsistencies) and advantages (innovation capacity, distributed resilience mechanisms) that affected different democratic systems in varying ways.

The integration of AI into information operations represents qualitative transformation in persuasion capabilities, though current limitations constrain operational effectiveness[661]. High-quality synthetic media generation requires substantial computational resources (approximately $2,000-5,000 per minute for convincing deepfake video), while AI-generated content continues exhibiting detectable statistical signatures when proper analysis tools are deployed. The COVID-19 pandemic provided insights into cognitive security challenges, revealing vulnerabilities in democratic information processing while demonstrating state-platform coordination possibilities. However, measuring the effectiveness of various countermeasures remains difficult due to the multiple variables affecting public health compliance and political outcomes.

The comparative analysis examines institutional capacity, societal resilience, and technological integration across the three cases, while acknowledging that different metrics may not be directly comparable across distinct political systems. Where quantitative comparisons are presented, they serve illustrative rather than definitive purposes, given the challenges of standardizing measurements across different institutional contexts and classification constraints affecting data availability.

---

[660] NATO Strategic Communications Centre of Excellence. "Russian Information Operations in Central Europe: Strategies and Countermeasures." Riga: NATO StratCom COE, 2023.

[661] Executive Office of the President. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." Washington, D.C.: The White House, October 30, 2023.

The United States exhibits institutional fragmentation that creates both coordination challenges and distributed resilience. Strategic communication activities span multiple agencies with combined annual budgets exceeding $2.3 billion[662], though coordination mechanisms remain constrained by constitutional separation of powers and federal structure requirements. Constitutional protections that limit domestic information operations create operational constraints compared to European allies. However, these same protections generate compensating advantages through enhanced civil society resilience and private sector innovation. The United States hosts over 200 independent fact-checking organizations[663], creating distributed defensive capacity that centralized approaches struggle to replicate. Without constitutional constraints, the U.S. might achieve faster crisis response coordination but could lose the legitimacy and innovation advantages that emerge from pluralistic information environments. The question becomes whether short-term operational efficiency justifies potential long-term costs to democratic legitimacy and adaptive capacity.

France's approach reflects institutional securitization through state-centric frameworks that prioritize rapid response and unified messaging. The creation of specialized units like VIGINUM and integration of information operations into military doctrine represent systematic institutional adaptation[664], though measuring operational effectiveness remains challenging due to classification constraints. French centralization enables rapid crisis response but creates potential vulnerabilities around democratic accountability and operational flexibility. The emphasis on republican universalism provides narrative coherence while creating tensions around identity-based grievances that malicious actors can exploit. French approaches depend on administrative traditions and political cultures that may not transfer to federal systems with different constitutional constraints and political traditions. The apparent success of centralized coordination must be evaluated within specific French institutional contexts rather than treated as universally applicable best practices.

Poland's strategic communication capabilities reflect rational adaptation to resource constraints and threat environments rather than institutional failure. Heavy reliance on NATO and EU frameworks provides access to sophisticated capabilities while requiring lower domestic

[662] Congressional Budget Office. "Federal AI Security Investment Analysis, FY 2025." Washington, D.C.: CBO, September 2024.
[663] First Draft. "State of the Field: Fact-Checking and Information Verification Organizations in North America." Cambridge, MA: First Draft, 2022.
[664] Ministère des Armées. *Stratégie d'Intelligence Artificielle de Défense*. Paris: République Française, 2022.

investment[665], though creating potential dependency vulnerabilities during crises when alliance consensus might be delayed. Polish civil society demonstrates significant independent capacity despite resource limitations[666], with local initiatives often exceeding national capabilities in specific domains. This bottom-up resilience aligns with NATO's emphasis on societal resilience while suggesting alternative approaches to capability development that do not require centralized state investment. Poland's apparent institutional weaknesses may reflect rational prioritization of conventional defense capabilities over information operations, given immediate territorial threats and available alliance support. Alternative resource allocation strategies might achieve different capability balances but would involve trade-offs across other security domains.

The research identifies limitations in traditional securitization theory when applied to information warfare contexts. Information threats often involve continuous, distributed processes rather than discrete crisis moments requiring immediate extraordinary measures. The concept of "graduated securitization" emerges from this analysis meaning an incremental expansion of state authority with maintained accountability mechanisms that may better capture democratic adaptation to persistent cognitive threats. However, this modification requires further theoretical development and empirical testing across additional cases to establish broader validity beyond the three countries examined here.

The analysis demonstrates that information warfare effectiveness depends significantly on target society characteristics rather than operational sophistication alone. Historical experience, institutional trust levels[667], and existing social divisions all mediate the impact of information campaigns, suggesting that defensive strategies should address underlying social conditions rather than focusing exclusively on technical countermeasures[668]. What appear as democratic "vulnerabilities" (openness, pluralism, transparency) may actually represent long-term strategic advantages that authoritarian competitors cannot replicate. The challenge

[665] Polish Academy of Sciences. "National AI Research Investment Report 2023." Warsaw: PAN, 2023.
[666] CBOS (Centrum Badania Opinii Społecznej). "Trust in Public Institutions 2023." Warsaw: CBOS, 2023.
[667] Edelman Trust Institute. *2023 Edelman Trust Barometer*. New York: Edelman, 2023.
[668] Government of Finland. "Security Strategy for Society: Government Resolution." Helsinki: Security Committee, 2017.

involves developing defensive capabilities that preserve these advantages while providing adequate protection against systematic manipulation[669].

The resilience framework reveals that institutional, societal, and technological dimensions can partially compensate for each other, though effective collective defense appears to require minimum threshold levels across all domains. This suggests that different democratic systems can achieve security through varying combinations of capabilities based on their specific constraints and advantages.

Information warfare analysis faces fundamental attribution problems that limit the strength of causal claims. While intelligence assessments provide valuable insights, establishing direct causal links between specific information campaigns and political outcomes remains analytically difficult. This thesis acknowledges these limitations rather than claiming definitive proof of operational effectiveness or failure.

The focus on post-1991 developments may not provide sufficient historical depth to support broader theoretical claims about democratic adaptation patterns. The four-period framework serves analytical convenience but may impose artificial periodization on more continuous evolutionary processes.

Quantitative metrics presented throughout the analysis should be interpreted as illustrative rather than definitive, given classification constraints, definitional inconsistencies across national contexts, and the inherent difficulty of measuring information warfare effectiveness. Future research should develop more robust measurement frameworks while acknowledging the persistent challenges in this domain.

The analysis suggests that effective democratic responses require balancing operational effectiveness, democratic legitimacy, and international credibility: three imperatives that often conflict with each other. Policy recommendations must account for implementation feasibility and potential unintended consequences rather than assuming optimal compliance and resource availability. Effective strategic communication coordination requires institutional authorities compatible with domestic constitutional frameworks. Importing best practices from different

[669] Roozenbeek, Jon, and Sander van der Linden. "Prebunking Interventions Based on 'Inoculation' Theory Can Reduce Susceptibility to Misinformation Across Cultures." *Harvard Kennedy School Misinformation Review* 1, no. 2 (2020): 1-23.

legal and political systems rarely works as intended and may undermine the legitimacy necessary for sustainable policy implementation. Civil society organizations provide cost-effective contributions to information resilience, but sustainable funding mechanisms remain problematic across all three cases examined. Different approaches (philanthropic, state-supported, EU-funded) involve distinct trade-offs between independence, sustainability, and political capture that require careful consideration. Regulatory approaches involve unavoidable trade-offs between security effectiveness and innovation capacity. Optimal frameworks must balance these competing objectives while accounting for rapid technological change that may outpace regulatory adaptation mechanisms. Policy recommendations should consider what might happen in the absence of proposed interventions. Enhanced state authority over information domains could provide security benefits but might also create new vulnerabilities through reduced innovation, decreased legitimacy, or authoritarian drift that adversaries could exploit through different strategies.

The convergence of AI with strategic communication creates new challenges that existing frameworks may not adequately address. However, technological determinism should be avoided. Social, political, and institutional factors will significantly mediate AI's impact on information warfare dynamics. Current AI systems face significant constraints that limit their strategic utility. Production costs, detection possibilities, and cultural adaptation challenges suggest that human-generated content will remain important for effective influence operations. Adversary capabilities should neither be underestimated nor overstated when developing defensive strategies. Democratic societies demonstrate learning capacity through institutional innovation and policy adaptation, though these processes operate on timescales that strategic competitors may exploit. The challenge involves accelerating democratic adaptation without compromising the deliberative processes that provide legitimacy and error-correction mechanisms.

This comparative analysis demonstrates that democratic societies face genuine challenges in adapting to information warfare while maintaining constitutional character. These challenges appear manageable given appropriate institutional innovation and sustained political commitment, though success requirements remain demanding and outcomes uncertain.

The most significant finding may be that effective democratic responses require patient institution-building rather than rapid technological fixes or comprehensive reorganization. Successful adaptations across all three cases developed incrementally through trial-and-error processes that enabled learning from experience while maintaining democratic accountability. Democratic systems exhibit both vulnerabilities and advantages in information warfare contexts. Constitutional constraints limit immediate response capabilities but may provide long-term advantages through legitimacy preservation and adaptive capacity. The relative importance of these factors depends on threat characteristics, time horizons, and strategic objectives that vary across different contexts.

Whether democratic societies can develop cognitive security frameworks that enhance collective decision-making capacity while preserving epistemic pluralism remains an open empirical question rather than a predetermined outcome. Success will likely depend on sustained political commitment, institutional creativity, and international cooperation that cannot be assumed given current political trends and resource constraints.

Future research should examine how these patterns extend to different democratic contexts while tracking institutional evolution as information threats continue developing. The framework developed here provides analytical tools while acknowledging significant uncertainties that constrain confident prediction about democratic adaptation to emerging technologies and evolving strategic competition in the information domain.

BIBLIOGRAPHY

Abernathy, Penelope Muse. *News Deserts and Ghost Newspapers: Will Local News Survive?* Chapel Hill: UNC Hussman School of Journalism and Media, 2020. https://www.usnewsdeserts.com/wp-content/uploads/2020/06/2020_News_Deserts_and_Ghost_Newspapers.pdf

Abrams, Floyd. *Speaking Freely: Trials of the First Amendment*. New York: Viking, 2005. Print.

Adler, Emanuel. "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control." *International Organization* 46, no. 1 (1992): 101-145. https://www.cambridge.org/core/journals/international-organization/article/abs/emergence-of-cooperation-national-epistemic-communities-and-the-international-evolution-of-the-idea-of-nuclear-arms-control/AD5AB338380EC8691C621B351BC11CE3

———. "Seizing the Middle Ground: Constructivism in World Politics." *European Journal of International Relations* 3, no. 3 (1997): 319-363. https://journals.sagepub.com/doi/10.1177/1354066197003003003

Afrobarometer. "African Perceptions of Foreign Powers: 2013-2021 Comparative Survey." Round 8 Survey Results, 2021. https://microdata.worldbank.org/index.php/catalog/4741

Agence Nationale de la Sécurité des Systèmes d'Information. "Attribution de l'Attaque Informatique contre la Campagne d'Emmanuel Macron." ANSSI Technical Report, May 2017. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

———. *Cybersécurité de l'Intelligence Artificielle*. Paris: République Française, 2021. Print.

Aldrich, Daniel P., and Michelle A. Meyer. "Social Capital and Community Resilience." *American Behavioral Scientist*5 9, no. 2 (2015): 254-269. https://www.academia.edu/19495313/Seizing_the_Middle_Ground_Constructivism_in_World_Politics

Algan, Yann, and Pierre Cahuc. "Trust and Growth." *Annual Review of Economics* 5, no. 1 (2013): 521-549. https://www.annualreviews.org/content/journals/10.1146/annurev-economics-081412-102108

Alliance for Securing Democracy. “Hamilton Dashboard.” Washington, D.C.: German Marshall Fund of the United States, 2022. https://securingdemocracy.gmfus.org/hamilton-dashboard/

———. “RT France and Russian Information Operations in Europe.” Washington, D.C.: German Marshall Fund, March 2019. Print.

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York: Longman, 1999. Print.

Allison, Roy. “Russia Resurgent? Moscow’s Campaign to ‘Coerce Georgia to Peace.’” *International Affairs* 84, no. 6 (2008): 1145-1171. https://commonweb.unifr.ch/artsdean/pub/gestens/f/as/files/4760/39349_201918.pdf

———. “Russian ‘Deniable’ Intervention in Ukraine: How and Why Russia Broke the Rules.” *International Affairs* 90, no. 6 (2014): 1255-1297. https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2346.12170

Amnesty International France. *Technologies de Surveillance et Droits Humains en France*. Paris: Amnesty International, 2022. Print.

Anderson, Benedict. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Rev. ed. London: Verso, 2006. Print.

Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 2005. Print.

Applebaum, Anne, and Peter Pomerantsev. “How to Put Out Democracy’s Dumpster Fire.” *The Atlantic*, March 2021. https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-to-be-awful/618079/

Arquilla, John, and David Ronfeldt. “The Advent of Netwar.” In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 1-25. Santa Monica, CA: RAND Corporation, 2001. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/RAND_MR1382.pdf

———. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation, 1997. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/RAND_MR880.pdf

Art, Robert J. *A Grand Strategy for America*. Ithaca, NY: Cornell University Press, 2003. https://www.jstor.org/stable/10.7591/j.ctt28547w

Art, Robert J., and Kenneth N. Waltz, eds. *The Use of Force: Military Power and International Politics*. 7th ed. Lanham, MD: Rowman & Littlefield, 2009. Print.

Arthur, W. Brian. "Competing Technologies, Increasing Returns, and Lock-In by Historical Events." *The Economic Journal* 99, no. 394 (1989): 116-131. https://www.jstor.org/stable/2234208

Assemblée Nationale. "Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République." *Journal Officiel de la République Française*, August 25, 2021. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043964778

———. "Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information." *Journal Officiel de la République Française*, December 23, 2018. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/

———. "Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025." *Journal Officiel de la République Française*, July 14, 2018. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037192797

———. "Proposition de loi relative à la lutte contre la manipulation de l'information." Session ordinaire 2017-2018, no. 799. Paris: Assemblée Nationale, March 21,2018. https://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_fausses_informations#-DEPOT

———. "Rapport d'information sur l'opération Artemis." Paris: Assemblée Nationale, December 2003. Print.

———. "Rapport d'Information sur l'Évaluation de la Politique de Prévention de la Radicalisation." Commission de la Défense Nationale et des Forces Armées. Paris: Assemblée Nationale, 2019. https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b2082_rapport-information

———. "Rapport de la Commission de la Défense Nationale et des Forces Armées sur l'Intelligence Artificielle." 16ème législature. Paris: Assemblée Nationale, 2022. Print.

———. "Rapport sur l'Agence Nationale de la Sécurité des Systèmes d'Information." Commission de la Défense. Paris: Assemblée Nationale, 2022. Print.

Association Française de Science Politique. "Enquête sur l'Autocensure dans la Recherche en Relations Internationales." AFSP Survey, 2023. Print.

Atkinson, Rick. *Crusade: The Untold Story of the Persian Gulf War*. Boston: Houghton Mifflin, 1993. Print.

Backes, Swen, and Alek Swab. "Cognitive Warfare: The Future of Cognitive Dominance." Riga: NATO Strategic Communications Centre of Excellence, 2019. https://www.belfercenter.org/sites/default/files/pantheon_files/2019-11/CognitiveWarfare.pdf

Badouard, Romain. "The Yellow Vests and the Politicization of Digital Platforms." *French Politics* 18, no. 2 (2020): 238-251. Print.

Badie, Bertrand. *L'Hégémonie Contestée: Les Nouvelles Formes de Domination Internationale*. Paris: Fayard, 2019. Print.

Bail, Christopher A., Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky. "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://www.pnas.org/doi/10.1073/pnas.1906420116

Baker, Andrew. "The Gradual Transformation of European Central Banking." *European Review of International Studies*1, no. 1 (2013): 3-28. Print.

Baldwin, David A., ed. *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press, 1993. https://cup.columbia.edu/book/neorealism-and-neoliberalism/9780231084413/

Balkin, Jack M. "Free Speech is a Triangle." *Columbia Law Review* 118, no. 7 (2018): 2011-2056. https://columbialawreview.org/content/free-speech-is-a-triangle/

Balzacq, Thierry. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1-30. London: Routledge, 2011. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203868508-8/theory-securitization-origins-core-assumptions-variants-thierry-balzacq

———. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11, no. 2 (2005): 171-201. https://journals.sagepub.com/doi/10.1177/1354066105052960

Bar-Yam, Yaneer. *Dynamics of Complex Systems*. Reading, MA: Addison-Wesley, 1997. https://fernandonogueiracosta.wordpress.com/wp-content/uploads/2015/08/yaneer-bar-yam-dynamics-of-complex-systems.pdf

Barrero, Jose Maria, Nicholas Bloom, and Steven J. Davis. "COVID-19 Is Also a Reallocation Shock." *Brookings Papers on Economic Activity* 2020, no. 2 (2020): 329-371. Print.

Bateman, Jon. "U.S. Foreign Policy and the AI Revolution." Washington, D.C.: Carnegie Endowment for International Peace, 2022. Print.

Beach, Derek, and Rasmus Brun Pedersen. *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor: University of Michigan Press, 2013. https://www.researchgate.net/publication/287260232_Process-Tracing_Methods_Foundations_and_Guidelines

Becker, Klaus, and Vivien Schmidt. "Institutional Development in New Democracies: Evolutionary vs. Revolutionary Pathways." *Comparative Political Studies* 54, no. 8 (2021): 1425-1456. Print.

Beitz, Charles R. *Political Theory and International Relations*. Princeton, NJ: Princeton University Press, 1979. https://archive.org/details/politicaltheoryi00beit/page/n7/mode/2up

Bellingcat Investigation Team. "FSB Documents on French Destabilization Operations." Bellingcat, December 2020. https://www.bellingcat.com/news/uk-and-europe/2020/12/03/proof-of-fsb-links-to-operations-against-france/

Bendiek, Annegret, and Tobias Wagner. "GAIA-X: A European Response to Digital Sovereignty?" SWP Comment 2021/C 07. Berlin: German Institute for International and Security Affairs, February 2021. Print.

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press, 1986. https://www.hup.harvard.edu/books/9780674169869

Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press, 2018. https://www.researchgate.net/publication/335317707_Network_Propaganda_Manipulation_Disinformation_and_Radicalization_in_American_Politics_By_Yochai_Benkler_Robert_Faris_and_Hal_Roberts_New_York_Oxford_University_Press_2018_472p_9900_cloth_2795_paper_-

Bennett, Andrew, and Jeffrey T. Checkel, eds. *Process Tracing: From Metaphor to Analytic Tool*. Cambridge: Cambridge University Press, 2015. https://www.cambridge.org/core/books/process-tracing/5BBC24CBF2E89114817741D0476C07A9

Bennett, W. Lance, and Steven Livingston. “The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions.” *European Journal of Communication* 33, no. 2 (2018): 122-139. https://journals.sagepub.com/doi/10.1177/0267323118760317

Bergen, Peter L. *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*. New York: Crown Publishers, 2012. Print.

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Garden City, NY: Anchor Books, 1966. https://amstudugm.wordpress.com/wp-content/uploads/2011/04/social-construction-of-reality.pdf

Bērziņa-Čerenkova, Una A. “China’s Digital Silk Road and Belt and Road Initiative: Connectivity, Influence and Governance.” *Chinese Journal of Communication* 15, no. 2 (2022): 215-234. Print.

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge, 2011. https://www.researchgate.net/publication/345705816_Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-power

Bigo, Didier. “Security and Immigration: Toward a Critique of the Governmentality of Unease.” *Alternatives* 27, no. 1 (2002): 63-92. https://journals.sagepub.com/doi/10.1177/03043754020270S105

Bijker, Wiebe E., Thomas P. Hughes, and Trevor J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987. https://www.jstor.org/stable/j.ctt5vjrsq

Bjola, Corneliu, and Marcus Holmes, eds. *Digital Diplomacy: Theory and Practice*. London: Routledge, 2015. https://www.routledge.com/Digital-Diplomacy-Theory-and-Practice/Bjola-Holmes/p/book/9781138843820?srsltid=AfmBOoowUrGgpSkVZk_U664zdzD5VoCkcNuuaHtTKhlWKwojdYqESS9q

Bjola, Corneliu, and Jen Wellings Papadakis. “Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience.” *Cambridge Review of International Affairs* 33, no. 5 (2020): 638-666. https://www.tandfonline.com/doi/abs/10.1080/09557571.2019.1704221

Boin, Arjen, Allan McConnell, and Paul 't Hart, eds. *Governing After Crisis: The Politics of Investigation, Accountability and Learning*. Cambridge: Cambridge University Press, 2008. https://www.researchgate.net/publication/46713001_Governing_After_Crisis_The_Politics_of_Investigation_Accountability_and_Learning

Boin, Arjen, and Michel J. G. van Eeten. "The Resilient Organization." *Public Administration* 91, no. 2 (2013): 429-445. https://www.researchgate.net/publication/261853574_The_Resilient_Organization

Bohas, Alexandre. *The New Franco-German Partnership and Europe*. London: Palgrave Macmillan, 2006. Print.

Bourdieu, Pierre, and Jean-Claude Passeron. *Reproduction in Education, Society and Culture*. London: Sage Publications, 1977. https://www.jstor.org/stable/3098926

Bovens, Mark. "Analysing and Assessing Accountability: A Conceptual Framework." *European Law Journal* 13, no. 4 (2007): 447-468. https://www.researchgate.net/publication/227681168_Analysing_and_Assessing_Accountability_A_Conceptual_Framework

Boyd, Danah. "Data Voids: Where Missing Data Can Easily Be Exploited." New York: Data & Society Research Institute, May 2018. https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf

Bozo, Frédéric. *Mitterrand, the End of the Cold War, and German Unification*. New York: Berghahn Books, 2009. Print.

Brachman, Jarret M. *Global Jihadism: Theory and Practice*. London: Routledge, 2009. https://www.start.umd.edu/publication/global-jihadism-theory-and-practice

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." Oxford Internet Institute Working Paper 2021.1. Oxford: Oxford Internet Institute, 2021. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/

Brady, Anne-Marie. "Magic Weapons: China's Political Influence Activities Under Xi Jinping." Washington, D.C.: Wilson Center, September 2017. https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping

Brandenburg v. Ohio, 395 U.S. 444 (1969). https://www.law.cornell.edu/supremecourt/text/395/444

Brehm, John, and Scott Gates. *Working, Shirking, and Sabotage: Bureaucratic Response to a Democratic Public*. Ann Arbor: University of Michigan Press, 1997. https://www.jstor.org/stable/10.3998/mpub.15149

Brennen, J. Scott, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen. "Types, Sources, and Claims of COVID-19 Misinformation." Oxford: Reuters Institute for the Study of Journalism, April 2020. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

Brooks, Stephen G., and William C. Wohlforth. *America Abroad: The United States' Global Role in the 21st Century*. New York: Oxford University Press, 2016. https://global.oup.com/academic/product/america-abroad-9780190464257?cc=gb&lang=en&

Brown, Tom B., Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, et al. "Language Models are Few-Shot Learners." *Advances in Neural Information Processing Systems* 33 (2020): 1877-1901. https://arxiv.org/pdf/2005.14165

Brubaker, Rogers. *Citizenship and Nationhood in France and Germany*. Cambridge, MA: Harvard University Press, 1992. https://www.jstor.org/stable/j.ctv26071qp

Buchanan, Ben, Andrew Lohn, Micah Musser, and Katerina Sedova. "Truth, Lies, and Automation: How Language Models Could Change Disinformation." Georgetown: Center for Security and Emerging Technology, May 2021. https://cset.georgetown.edu/publication/truth-lies-and-automation/

Bundesnachrichtendienst. "Bilateral Intelligence Assessment: French Information Operations." BND Report, 2023 (excerpts declassified). Print.

Buzan, Barry, and Ole Wæver. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003. https://www.cambridge.org/core/books/regions-and-powers/9E0B611D4C01CECD704651B273646E1D

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers, 1998. Print.

Calo, Ryan. "Robotics and the Lessons of Cyberlaw." *California Law Review* 103, no. 3 (2015): 513-563. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1022&context=faculty-articles

Campbell, David. *Writing Security: United States Foreign Policy and the Politics of Identity*. Minneapolis: University of Minnesota Press, 1992. https://manchesteruniversitypress.co.uk/9780719055492/

Campbell, Donald T. "Reforms as Experiments." *American Psychologist* 24, no. 4 (1969): 409-429. https://www.sfu.ca/~palys/Campbell-1969-ReformsAsExperiments.pdf

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, eds. *Cyberwar: Security, Strategy and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press, 1996. https://archive.org/details/cyberwar0000unse/page/12/mode/2up

Camus, Jean-Yves, and Nicolas Lebourg. *Les Droites Extrêmes en Europe*. Paris: Le Seuil, 2017. Print.

Carpenter, Daniel P., and David A. Moss, eds. *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*. Cambridge: Cambridge University Press, 2014. https://www.cambridge.org/core/books/preventing-regulatory-capture/4DF3FC5A3202552A18F3D41835D46833

Casilli, Antonio A., and Dominique Cardon. "Digital Sovereignty: A Critical Approach." *Internet Policy Review* 11, no. 2 (2022): 1-21. Print.

Castells, Manuel. *Communication Power*. Oxford: Oxford University Press, 2009. Print.

———. *The Rise of the Network Society*. 2nd ed. Oxford: Blackwell Publishers, 2009. https://onlinelibrary.wiley.com/doi/book/10.1002/9781444319514

Castex, Jean. "Création du Service VIGINUM." Décret n° 2021-930. *Journal Officiel de la République Française*, July 13, 2021. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361

CBOS (Centrum Badania Opinii Społecznej). "Polish Attitudes Toward Ukraine Crisis: Longitudinal Analysis 2022-2023." Warsaw: CBOS, 2024. https://www.cbos.pl/PL/publikacje/public_opinion/2023/09_2023.pdf

———. "Polish Public Opinion on Border Security." Warsaw: CBOS, December 2021. https://www.cbos.pl/PL/publikacje/public_opinion/2021/12_2021.pdf

———. "Trust in Public Institutions 2023." Warsaw: CBOS, 2023. https://www.cbos.pl/PL/publikacje/public_opinion/2023/01_2023.pdf

Celeste, Edoardo. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology* 33, no. 1 (2019): 76-99.

https://www.researchgate.net/publication/330135709_Digital_constitutionalism_a_new_systematic_theorisation

Center for Strategic and International Studies. *Strategic Competition in an Era of Artificial Intelligence*. Washington, D.C.: CSIS, 2021. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence

CEVIPOF. "Baromètre de la Confiance Politique 2023." Paris: Sciences Po, 2023. https://www.sciencespo.fr/cevipof/fr/etudes-enquetes/barometre-confiance-politique/

Chadwick, Andrew. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press, 2013. https://academic.oup.com/book/8696?searchresult=1

Charap, Samuel. "The Ghost of Hybrid War." *Survival* 57, no. 6 (2015): 51-68. https://ir101.co.uk/wp-content/uploads/2018/05/charap-2015-the-ghost-of-hybrid-war.pdf

Charon, Paul, and Jean-Baptiste Jeangène Vilmer. "Chinese Influence Operations: A Machiavellian Moment." IRSEM Research Paper No. 64. Paris: Institute for Strategic Research, October 2021. https://www.researchgate.net/publication/367252670_Chinese_Influence_Operations_A_Machiavellian_Moment

Checkel, Jeffrey T. "The Constructivist Turn in International Relations Theory." *World Politics* 50, no. 2 (1998): 324-348. https://www.jstor.org/stable/25054040

Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753-1820. https://scholarship.law.bu.edu/faculty_scholarship/640/

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984. https://icct.nl/sites/default/files/import/publication/On-War.pdf

Coalition for Content Provenance and Authenticity. "C2PA Technical Specification." Version 1.3. C2PA Working Group, 2023. https://spec.c2pa.org/specifications/specifications/2.2/index.html

Collier, David. "Understanding Process Tracing." *PS: Political Science & Politics* 44, no. 4 (2011): 823-830. https://polisci.berkeley.edu/sites/default/files/people/u3827/Understanding%20Process%20Tracing.pdf

Commission Nationale de Contrôle de la Campagne Électorale en vue de l'Élection Présidentielle. "Communiqué concernant la Diffusion de Documents Piratés." Paris: CNCCEP, May 5, 2017. https://www.cnccep.fr/pdf-cp11.html

Commission Nationale de l'Informatique et des Libertés. *Rapport d'Activité 2021*. Paris: CNIL, 2021. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf

Commission Nationale du Débat Public. *Intelligence Artificielle et Participation Citoyenne*. Paris: CNDP, 2021. Print.

Communications Decency Act of 1996, 47 U.S.C. § 230. https://www.law.cornell.edu/uscode/text/47/230

Congressional Budget Office. "Federal AI Security Investment Analysis, FY 2025." Washington, D.C.: CBO, September 2024. Print.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." Arlington, VA: CNA Corporation, March 2017. https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf

Constitutional Tribunal of the Republic of Poland. "Ruling K 1/21 regarding Constitutional Boundaries of Information Policy." Warsaw: Constitutional Tribunal, 2021. https://siecobywatelska.pl/explanatory-memorandum-on-polish-foia-constitutional-case-k1-21/?lang=en

Cook, Thomas D., and Donald T. Campbell. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*. Boston: Houghton Mifflin, 1979. https://archive.org/details/quasiexperimenta00cook

Coquard, Benoît. *Ceux qui Restent: Faire sa Vie dans les Campagnes en Déclin*. Paris: La Découverte, 2019. https://journals.openedition.org/sociologie/10469

Cordesman, Anthony H. "The Afghan War Is Over, But Information War Continues." Washington, D.C.: Center for Strategic and International Studies, September 2021. Print.

Cornish, Paul, Julian Lindley-French, and Claire Yorke. "Strategic Communications and National Strategy." London: Chatham House, September 2011. https://www.chathamhouse.org/sites/default/files/r0911stratcomms.pdf

Cour des Comptes. *Les Moyens de la Communication Gouvernementale*. Paris: Cour des Comptes, 2023. Print.

Cullen, Patrick J., and Erik Reichborn-Kjennerud. “Understanding Hybrid Warfare.” MCDC Countering Hybrid Warfare Project, 2017. https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

Cull, Nicholas J. *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989*. Cambridge: Cambridge University Press, 2008. https://www.cambridge.org/core/books/cold-war-and-the-united-states-information-agency/464FCD1CF9C551AD461D11EB3924F6D2

Culpepper, Pepper D. *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. Cambridge: Cambridge University Press, 2011. https://www.cambridge.org/core/books/quiet-politics-and-business-power/56127E2EE022EBA207A337E49BFD16B5

CyberSec EXPO. *Post-Event Analysis Report 2022-2023*. Katowice: Cybersec Foundation, 2023. Print.

Cybersecurity and Infrastructure Security Agency. *2020 Election Security: Ensuring Success*. Washington, D.C.: Department of Homeland Security, 2021. Print.

Dahl, Robert A. *Democracy and Its Critics*. New Haven, CT: Yale University Press, 1989. https://www.jstor.org/stable/1289333

Darczewska, Jolanta. “The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.” Centre for Eastern Studies Point of View 42. Warsaw: Centre for Eastern Studies, 2014. https://www.files.ethz.ch/isn/181102/PW42_the_anatomy_of_russian_information_warfare.pdf

Darr, Joshua P., Matthew P. Hitt, and Johanna L. Dunaway. “Newspaper Closures Polarize Voting Behavior.” *Journal of Communication* 68, no. 6 (2018): 1007-1028. https://academic.oup.com/joc/article-abstract/68/6/1007/5160090?redirectedFrom=fulltext

Defense Advanced Research Projects Agency. “Media Forensics (MediFor).” Arlington, VA: DARPA, 2023. https://www.darpa.mil/research/programs/media-forensics

———. “Semantic Forensics (SemaFor).” Arlington, VA: DARPA, 2023. https://www.darpa.mil/research/programs/semantic-forensics

Deibert, Ronald J. “The Road to Digital Unfreedom: Three Painful Truths about Social Media.” *Journal of Democracy* 30, no. 1 (2019): 25-39. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/

Délégation Générale pour l’Armement - Direction de la Stratégie. *Intelligence Artificielle et Autonomie des Systèmes d’Armes*. Paris: République Française, 2021. Print.

Deltombe, Thomas. *L’Islam Imaginaire: La Construction Médiatique de l’Islamophobie en France, 1975-2005*. Paris: La Découverte, 2005. Print.

Demagog.org.pl. *Annual Report 2023: Fact-Checking in Poland*. Warsaw: Demagog Foundation, 2023. https://demagog.org.pl/wp-content/uploads/2024/05/Sprawozdanie-finansowe-Demagog-2023.pdf

DeNardis, Laura. *The Global War for Internet Governance*. New Haven, CT: Yale University Press, 2020. https://www.jstor.org/stable/j.ctt5vkz4n

Denzin, Norman K. *The Research Act: A Theoretical Introduction to Sociological Methods*. 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1989. https://archive.org/details/researchacttheo00denz

Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” Washington, D.C.: Department of Defense, July 2011. https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf

———. “DOD Data Strategy.” Washington, D.C.: Department of Defense, 2022. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

———. “Quadrennial Defense Review Report.” Washington, D.C.: Department of Defense, 2006. Print.

———. “Strategic Communication Guidance Memorandum.” Washington, D.C.: Department of Defense, 2006. https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2006.pdf?ver=2014-06-25-111017-150

Der Derian, James. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. 2nd ed. New York: Routledge, 2009. https://www.routledge.com/Virtuous-War-Mapping-the-Military-Industrial-Media-Entertainment-Network/DerDerian/p/book/9780415772396?srsltid=AfmBOopueIYRT2jvYQ0t8YF3K-SYMLYY1TDe3DH1hdRCPazHCoPbgM9P

Diamond, Larry. *Developing Democracy: Toward Consolidation*. Baltimore: Johns Hopkins University Press, 1999. Print.

———. "Liberation Technology." *Journal of Democracy* 21, no. 3 (2010): 69-83. https://www.journalofdemocracy.org/articles/liberation-technology/

DiMaggio, Paul J., and Walter W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48, no. 2 (1983): 147-160. https://www.jstor.org/stable/2095101

Ding, Jeffrey. "Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI." Oxford: Future of Humanity Institute, University of Oxford, 2018. Print.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics and Tropes of the Internet Research Agency." New York: New Knowledge, December 2018. https://digitalcommons.unl.edu/senatedocs/2/

Direction Générale de la Sécurité Intérieure. *Rapport sur les Mouvements de Contestation Sociale et les Ingérences Étrangères*. Paris: République Française, 2019. Print.

Donnelly, Christopher. "Defence Transformation in the New Democracies: A Framework for Tackling the Problem." *NATO Review* 45, no. 1 (1997): 15-19. https://procon.bg/article/defense-transformation-new-democracies-framework-tackling-problem

Doyle, Michael W. "Liberalism and World Politics." *American Political Science Review* 80, no. 4 (1986): 1151-1169. https://www.jstor.org/stable/1960861

Drezner, Daniel W. "The Power and Peril of International Regime Complexity." *Perspectives on Politics* 7, no. 1 (2009): 65-70. https://www.jstor.org/stable/40407216

Duffield, J. S. "NATO's Functions after the Cold War." *Political Science Quarterly* 109, no. 5 (1994): 763-787. https://www.jstor.org/stable/2152531

Dworkin, Ronald. *Taking Rights Seriously*. Cambridge, MA: Harvard University Press, 1977. https://scholarship.law.edu/cgi/viewcontent.cgi?article=2438&context=lawreview

Dyson, Kenneth H.F. *The State Tradition in Western Europe*. Oxford: Martin Robertson, 1980. https://archive.org/details/statetraditionin0000dyso

Easterly, Jen. "Testimony Before the House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection." U.S. House of Representatives, April 2024. https://docs.house.gov/meetings/AP/AP15/20240430/117210/HHRG-118-AP15-Wstate-EasterlyJ-20240430.pdf

Easton, David. *A Systems Analysis of Political Life*. New York: John Wiley & Sons, 1965. https://onlinelibrary.wiley.com/doi/abs/10.1002/bs.3830130208

Edelman Trust Institute. *2022 Edelman Trust Barometer*. New York: Edelman, 2022. https://www.edelman.com/trust/2022-trust-barometer

———. *2023 Edelman Trust Barometer*. New York: Edelman, 2023. https://www.edelman.com/trust/2023/trust-barometer

Edwards, Bob, and Michael W. Foley. "Civil Society and Social Capital Beyond Putnam." *American Behavioral Scientist*42, no. 1 (1998): 124-139. https://journals.sagepub.com/doi/10.1177/0002764298042001010

Ekiert, Grzegorz, and Jan Kubik. *Rebellious Civil Society: Popular Protest and Democratic Consolidation in Poland, 1989-1993*. Ann Arbor: University of Michigan Press, 1999. https://www.jstor.org/stable/10.3998/mpub.16117

En Marche! "Déclaration sur les Risques d'Ingérence Électorale." Communiqué de Campagne, February 2017. Print.

Entman, Robert M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43, no. 4 (1993): 51-58. https://www.researchgate.net/publication/209409849_Framing_Toward_Clarification_of_A_Fractured_Paradigm

Estonian Defence League. *Civil Cyber Defence Strategy 2022-2026*. Tallinn: Estonian Defence League, 2022. Print.

EUvsDisinfo. "The Kremlin this Week: Let's hate Poland!" January 23, 2020. https://euvsdisinfo.eu/the-kremlin-this-week-lets-hate-poland/

Evanega, Sarah, Mark Lynas, Jordan Adams, and Karinne Smolenyak. “Coronavirus Misinformation: Quantifying Sources and Themes in the COVID-19 ‘Infodemic.’” Ithaca, NY: Cornell Alliance for Science, July 2020. https://allianceforscience.org/wp-content/uploads/2020/09/Evanega-et-al-Coronavirus-misinformationFINAL.pdf

European Centre for AI Safety. “Synthetic Media Detection: Technical Assessment 2024.” Brussels: ECAIS, 2024. Print.

European Centre of Excellence for Countering Hybrid Threats. “Hybrid Threats as a Phenomenon.” Helsinki: Hybrid CoE, 2019. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

———. “The Finnish Model for Countering Hybrid Threats.” Helsinki: Hybrid CoE, 2018. Print.

European Commission. “2023 Rule of Law Report: Country Chapter on the Rule of Law Situation in Poland.” Brussels: European Commission, July 2023. https://commission.europa.eu/publications/2023-rule-law-report-communication-and-country-chapters_en

———. “Artificial Intelligence Act: Implementation Strategies Across Member States.” Brussels: European Commission, 2024. https://artificialintelligenceact.eu/national-implementation-plans/

———. “Code of Practice on Disinformation: Assessment Report.” Brussels: European Commission, 2021. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en

———. “Digital Education Action Plan 2021-2027.” Brussels: European Commission, 2021. https://education.ec.europa.eu/focus-topics/digital-education/actions

———. “Digital Europe Programme 2021-2027.” Brussels: European Commission, 2021. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

———. “Europe’s Digital Decade: Digital Targets for 2030.” Brussels: European Commission, 2021. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

———. “Media Literacy and Digital Citizenship: Cost-Effectiveness Analysis.” Brussels: European Commission, 2023. Print.

———. “Media Literacy Best Practices Report: Local Initiatives in EU Member States.” Brussels: European Commission, 2023. Print

———. “Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).” Brussels: European Commission, June 2023. https://artificialintelligenceact.eu/the-act/

European Council. “Council Conclusions on Countering Hybrid Threats.” Brussels: European Council, June 19, 2015. https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

———. “EU Restrictive Measures in Response to the Crisis in Belarus.” Brussels: European Council, 2021. https://www.consilium.europa.eu/en/policies/sanctions-against-belarus/

European External Action Service. “Questions and Answers about the East StratCom Task Force.” Brussels: EEAS, March 2019. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

———. “Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic.” EUvsDisinfo Special Report. Brussels: EEAS, 2021. https://www.eeas.europa.eu/delegations/georgia/eeas-special-report-update-short-assessment-narratives-and-disinformation-around-covid-19-pandemic_und_en

European External Action Service East StratCom Task Force. “Russian Disinformation and the Yellow Vests.” EUvsDisinfo Report. Brussels: EEAS, December 2019. https://euvsdisinfo.eu/figures-of-the-week-37/

Executive Office of the President. “Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People.” Washington, D.C.: The White House, October 2022. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

———. “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” Washington, D.C.: The White House, October 30, 2023. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Export Administration Regulations, 15 C.F.R. Parts 730-774 (2023). https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-730

Facon, Isabelle. “Russia’s National Security Strategy and Military Doctrine and Their Implications for the EU.” European Parliament Directorate-General for External Policies Policy Department Study EXPO/B/SEDE/2016/02. Brussels: European Parliament, May 2017. https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf

Farrell, Henry, and Abraham Newman. “Weaponized Interdependence: How Global Economic Networks Shape State Coercion.” *International Security* 44, no. 1 (2019): 42-79. https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic

Favell, Adrian. *Philosophies of Integration: Immigration and the Idea of Citizenship in France and Britain*. 2nd ed. Basingstoke, UK: Palgrave Macmillan, 2001. https://archive.org/details/philosophiesofin0002fave

Feaver, Peter D. *Armed Servants: Agency, Oversight, and Civil-Military Relations*. Cambridge, MA: Harvard University Press, 2003. https://www.jstor.org/stable/48608701

Federal Bureau of Investigation. “Iranian Cyber Group Emennet Pasargad Indicted for Threatening U.S. Voters, Disseminating False Election Information.” FBI Press Release, November 18, 2021. Print.

Ferrara, Emilio. “The History of Digital Spam.” *Communications of the ACM* 62, no. 8 (2019): 82-91. https://dl.acm.org/doi/10.1145/3299768

Finnish Government. “Finland’s Comprehensive Security Model.” Prime Minister’s Office Publications 2021/4. Helsinki: Prime Minister’s Office, 2021. https://turvallisuuskomitea.fi/en/comprehensive-security/

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52, no. 4 (1998): 887-917. https://www.jstor.org/stable/2601361

FireEye. “APT28: A Window into Russia’s Cyber Espionage Operations?” Milpitas, CA: FireEye, October 2017. Print.

———. “Iranian Influence Operation Leverages Network of Inauthentic News Sites and Social Media Targeting Audiences in U.S., UK, Latin America, Middle East.” Milpitas, CA: FireEye, August 2020. Print.

First Draft. “State of the Field: Fact-Checking and Information Verification Organizations in North America.” Cambridge, MA: First Draft, 2022. Print.

Floridi, Luciano. “Information Ethics: On the Philosophical Foundation of Computer Ethics.” *Ethics and Information Technology* 1, no. 1 (1999): 37-56. https://link.springer.com/article/10.1023/A:1010018611096

———. “Translating Urgency into Impact: Digital Ethics as a Political Force.” *Philosophy & Technology* 32, no. 4 (2019): 669-200. https://www.researchgate.net/publication/355881285_Translating_Principles_into_Practices_of_Digital_Ethics_Five_Risks_of_Being_Unethical

Flyvbjerg, Bent. “What You Should Know About Megaprojects and Why: An Overview.” *Project Management Journal*45, no. 2 (2014): 6-19. https://www.researchgate.net/publication/261411676_What_You_Should_Know_About_Megaprojects_and_Why_An_Overview

France Médias Monde. *Étude d’Impact en Afrique Francophone 2020-2023*. Paris: FMM, 2023. Print.

Freedman, Lawrence. “Information, Disinformation and Political Warfare.” In *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, Brian Mazanec, and Brandon Valeriano, 15-32. London: Routledge, 2019. Print.

———. “The Transformation of Strategic Affairs.” *Adelphi Paper* 379 (2006): 7-100. https://www.taylorfrancis.com/books/mono/10.4324/9780203820001/transformation-strategic-affairs-lawrence-freedman

Fridman, Ofer. “Hybrid Warfare or Gibridnaya Voyna?” *The RUSI Journal* 162, no. 1 (2017): 42-49. https://www.tandfonline.com/doi/full/10.1080/03071847.2016.1253370

Friedman, Milton. *Free to Choose: A Personal Statement*. New York: Harcourt Brace Jovanovich, 1980. https://periferiaactiva.wordpress.com/wp-content/uploads/2019/07/free-to-choose_-a-personal-statement.pdf

Frontex. “Risk Analysis for 2022.” Warsaw: European Border and Coast Guard Agency, 2022. https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/ARA_2022_Public_Web.pdf

Fukuyama, Francis. *America at the Crossroads: Democracy, Power, and the Neoconservative Legacy*. New Haven, CT: Yale University Press, 2006. https://archive.org/details/americaatcrossro0000fuku

———. *The End of History and the Last Man*. New York: Free Press, 1992. https://ia803100.us.archive.org/33/items/THEENDOFHISTORYFUKUYAMA/THE%20END%20OF%20HISTORY%20-%20FUKUYAMA.pdf

———. "The End of History?" *The National Interest* 16 (1989): 3-18. https://www.jstor.org/stable/24027184

Gaddis, John Lewis. *The Cold War: A New History*. New York: Penguin Press, 2005. https://ia803100.us.archive.org/33/items/thecoldwaranewhistory/The%20Cold%20War%20%20a%20new%20history.pdf

Gailmard, Sean, and John W. Patty. *Learning While Governing: Expertise and Accountability in the Executive Branch*. Chicago: University of Chicago Press, 2013. https://press.uchicago.edu/ucp/books/book/chicago/L/bo14365173.html

Galeotti, Mark. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security* 7, no. 2 (2019): 157-161. https://www.researchgate.net/publication/323450532_The_mythical_'Gerasimov_Doctrine'_and_the_language_of_threat

Gallup. "Confidence in Institutions." Princeton, NJ: Gallup, 2023. https://news.gallup.com/poll/1597/confidence-institutions.aspx

Gao, Pengjie, Chang Lee, and Dermot Murphy. "Financing Dies in Darkness? The Impact of Newspaper Closures on Public Finance." *Journal of Financial Economics* 135, no. 2 (2020): 445-467. https://www.sciencedirect.com/science/article/abs/pii/S0304405X19301606

Garrett, R. Kelly, and Shannon Poulsen. "Echo Chambers Online?: Politically Motivated Selective Exposure among Internet News Users." *Journal of Computer-Mediated Communication* 14, no. 2 (2019): 265-285. https://academic.oup.com/jcmc/article/14/2/265/4582957

Geddes, Barbara. "How the Cases You Choose Affect the Answers You Get: Selection Bias in Comparative Politics." *Political Analysis* 2 (1990): 131-150. https://www.cambridge.org/core/journals/political-analysis/article/abs/how-the-cases-you-choose-affect-the-answers-you-get-selection-bias-in-comparative-politics/05E854AA55C1BF090B56CEC73ACEFC6B

Georgetown Center for Security and Emerging Technology. "Chinese AI Research Investment Trends 2022-2024." CSET Data Brief. Georgetown: CSET, 2024. Print.

George, Alexander L. "The Case for Multiple Advocacy in Making Foreign Policy." *American Political Science Review* 66, no. 3 (1972): 751-785. https://www.jstor.org/stable/1957476

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005. https://mitpress.mit.edu/9780262572224/case-studies-and-theory-development-in-the-social-sciences/

Gerasimov, Valery. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations." *Military-Industrial Courier*, February 27, 2013. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016. https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

Giles, Keir, and Anthony Himebauch. "Handbook of Russian Information Warfare." Rome: NATO Defence College, November 2019. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

Gillespie, Tarleton. "Content Moderation, AI, and the Question of Scale." *Big Data & Society* 7, no. 2 (2020): 1-13. https://journals.sagepub.com/doi/full/10.1177/2053951720943234

———. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press, 2018. https://www.researchgate.net/publication/327186182_Custodians_of_the_internet_Platforms_content_moderation_and_the_hidden_decisions_that_shape_social_media

Goldberg, Matthew H., et al. "Social Norms Motivate COVID-19 Preventive Behaviors." *PsyArXiv* (2020): 1-25. https://www.researchgate.net/profile/Sander-Van-Der-Linden/publication/341135999_Social_norms_motivate_COVID-19_preventive_behaviors/links/5eb5973792851cd50da382a6/Social-norms-motivate-COVID-19-preventive-behaviors.pdf

Goldenberg, Ilan. "Iranian Hybrid Warfare: Implications for Future Conflict." Washington, D.C.: Center for a New American Security, March 2020. Print.

Goldfarb, Avi, and Jon Lindsay. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46, no. 3 (2022): 7-50. https://direct.mit.edu/isec/article/46/3/7/109668/Prediction-and-Judgment-Why-Artificial

Goldgeier, J. M. *Not Whether But When: The U.S. Decision to Enlarge NATO*. Washington, D.C.: Brookings Institution Press, 1999. https://www.jstor.org/stable/10.7864/j.ctvj7wm83

Goldstein, Frank L., and Benjamin F. Findley Jr., eds. *Psychological Operations: Principles and Case Studies*. Maxwell Air Force Base, AL: Air University Press, 1996. https://apps.dtic.mil/sti/tr/pdf/ADA316643.pdf

Goldstein, Josh A., Girish Sastry, Micah Musser, Renee DiResta, Matthew Scherer, and Dan Ryder. "Forecasting Potential Misuses of Language Models for Disinformation Campaigns and How to Reduce Risk." San Francisco: OpenAI, January 2023. https://cyber.fsi.stanford.edu/io/news/forecasting-potential-misuses-language-models-disinformation-campaigns-and-how-reduce-risk

———. "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations." Stanford, CA: Stanford Internet Observatory, January 2023. https://cyber.fsi.stanford.edu/io/publication/generative-language-models-and-automated-influence-operations-emerging-threats-and

Google AI. "FaceForensics++: Learning to Detect Manipulated Facial Images." In *Proceedings of the IEEE International Conference on Computer Vision*, 1-10. Los Alamitos, CA: IEEE, 2019. https://www.researchgate.net/publication/330672957_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images

Gordon, Philip H. *A Certain Idea of France: French Security Policy and the Gaullist Legacy*. Princeton, NJ: Princeton University Press, 1993. https://www.jstor.org/stable/j.ctt7s90s

Gordon, Philip H., and Jeremy Shapiro. *Allies at War: America, Europe, and the Crisis over Iraq*. New York: McGraw-Hill, 2004. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2208&context=nwc-review

Government of Finland. "Security Strategy for Society: Government Resolution." Helsinki: Security Committee, 2017. https://julkaisut.valtioneuvosto.fi/handle/10024/166026

Government Cybersecurity Strategy, Republic of Poland. *National Cybersecurity Strategy 2022-2027*. Warsaw: Prime Minister's Chancellery, 2022. Print.

GovTech Polska. *Annual Report 2023: Digital Transformation Initiatives*. Warsaw: Prime Minister's Chancellery, 2023. https://piit.org.pl/wp-content/uploads/2023/09/DDR2023_Poland_country_report.pdf

———. *Strategic Plan 2022-2025: Digital Innovation for Public Services*. Warsaw: Prime Minister's Chancellery, 2022. Print.

Granjon, Marie-Christine. “L’Afrique Francophone Face aux Nouvelles Guerres de l’Information.” *Politique Africaine* 160, no. 4 (2020): 85-107. Print.

Gray, Colin S. *Modern Strategy*. Oxford: Oxford University Press, 1999. https://global.oup.com/ukhe/product/modern-strategy-9780198782513?cc=gb&lang=en&

Grigas, Agnia. *Beyond Crimea: The New Russian Empire*. New Haven, CT: Yale University Press, 2016. https://academic.oup.com/yale-scholarship-online/book/14414

Gross, Peter. *Entangled Evolutions: Media and Democratization in Eastern Europe*. Washington, D.C.: Woodrow Wilson Center Press, 2002. https://www.wilsoncenter.org/book/entangled-evolutions-media-and-democratization-eastern-europe

Grzymala-Busse, Anna. *Rebuilding Leviathan: Party Competition and State Exploitation in Post-Communist Democracies*. Cambridge: Cambridge University Press, 2007. https://www.cambridge.org/core/books/rebuilding-leviathan/1E7ED3A562E8D10FD3AA0D6395C8A4FE

Guess, Andrew M., Brendan Nyhan, and Jason Reifler. “Exposure to Untrustworthy Websites in the 2016 US Election.” *Nature Human Behaviour* 4, no. 5 (2020): 472-480. https://www.nature.com/articles/s41562-020-0833-x

Guzzini, Stefano. “A Reconstruction of Constructivism in International Relations.” *European Journal of International Relations* 6, no. 2 (2000): 147-182. https://www.researchgate.net/publication/238164116_A_Reconstruction_of_Constructivism_in_International_Relations

Haas, Peter M. “Introduction: Epistemic Communities and International Policy Coordination.” *International Organization* 46, no. 1 (1992): 1-35. https://www.jstor.org/stable/2706951

Habermas, Jürgen. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: MIT Press, 1989. https://mitpress.mit.edu/9780262581080/the-structural-transformation-of-the-public-sphere/

Hagège, Claude. *Combat pour le français: Au nom de la diversité des langues et des cultures*. Paris: Odile Jacob, 2006. Print.

Hall, Peter A., and Rosemary C.R. Taylor. “Political Science and the Three New Institutionalisms.” *Political Studies* 44, no. 5 (1996): 936-957. https://journals.sagepub.com/doi/10.1111/j.1467-9248.1996.tb00343.x

Hallahan, Kirk, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič, and Krishnamurthy Sriramesh. "Defining Strategic Communication." *International Journal of Strategic Communication* 1, no. 1 (2007): 3-35. https://www.researchgate.net/publication/241730557_Defining_Strategic_Communication

Hallin, Daniel C., and Paolo Mancini. *Comparing Media Systems: Three Models of Media and Politics*. Cambridge: Cambridge University Press, 2004. https://www.cambridge.org/core/books/comparing-media-systems/B7A12371782B7A1D62BA1A72C1395E43

Halper, Stefan. "China: The Three Warfares." Washington, D.C.: U.S. Office of Net Assessment, May 2013. https://aul.primo.exlibrisgroup.com/discovery/fulldisplay/alma995281443406836/01AUL_INST:AUL

Hamilton 68. "Russian Information Operations Dashboard: Poland Migration Crisis Analysis." Washington, D.C.: Alliance for Securing Democracy, 2022. Print.

Hansen, Lene. "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School." *Millennium: Journal of International Studies* 29, no. 2 (2000): 285-306. https://journals.sagepub.com/doi/abs/10.1177/03058298000290020501

Harris Interactive. "Les Français et la Recherche Publique: Sondage d'Opinion." Paris: Harris Interactive France, Féebruary 2024. https://harris-interactive.fr/opinion_polls/barometre-de-confiance-politique-fevrier-2024/

Headquarters, Department of the Army. *Field Manual 3-24: Counterinsurgency*. Washington, D.C.: Department of the Army, 2006. https://www.bits.de/NRANEU/others/amd-us-archive/fm3-24fd06.pdf

Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari, and Andrej Zwitter. "Will Democracy Survive Big Data and Artificial Intelligence?" *Scientific American* 25 (2017): 1-8. https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

Helliwell, John F., Richard Layard, Jeffrey D. Sachs, and Jan Emmanuel De Neve, eds. *World Happiness Report 2021*. New York: Sustainable Development Solutions Network, 2021. https://www.worldhappiness.report/ed/2021/

Henrotin, Joseph. "L'Intelligence Artificielle de Défense en France: Enjeux et Perspectives." *Défense & Sécurité Internationale* 151 (2021): 42-47. Print.

Henrotin, Joseph. “La guerre cognitive: un nouveau champ de bataille?” *Défense & Sécurité Internationale* 154 (2020): 52-57. Print.

Herman, Edward S., and Noam Chomsky. *Manufacturing Consent: The Political Economy of the Mass Media*. New York: Pantheon Books, 1988. https://files.libcom.org/files/2022-04/manufacturing_consent.pdf

Hersh, Seymour M. “Torture at Abu Ghraib.” *The New Yorker*, May 10, 2004. https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49-60. https://www.jstor.org/stable/26463926?seq=1

Hoffman, Frank G. “Conflict in the 21st Century: The Rise of Hybrid Wars.” Arlington, VA: Potomac Institute for Policy Studies, 2007. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hoffman, Samantha, Elise Thomas, Fergus Ryan, and Jacob Wallis. “The Global Engagement Center vs. Chinese Propaganda.” Canberra: Australian Strategic Policy Institute, September 2020. https://www.ciaonet.org/catalog?per_page=100&sort=year&format=html&f%5Blocation%5D%5B%5D=Asia&f%5Bcontent_type%5D%5B%5D=Special+Report&f%5Binstitution%5D%5B%5D=Australian+Strategic+Policy+Institute+%28ASPI%29&f%5Bpub_date%5D%5B%5D=years_5&searched=yes&search_field=all_fields&q=Samantha+Hoffman

Hoffmann, Stanley. “The French National Style.” *In Search of France*, edited by Stanley Hoffmann, 3-27. Cambridge, MA: Harvard University Press, 1963. Print.

Holling, C.S. “Resilience and Stability of Ecological Systems.” *Annual Review of Ecology and Systematics* 4 (1973): 1-23. https://www.jstor.org/stable/2096802

Hopf, Ted. “The Promise of Constructivism in International Relations Theory” *International Security* 23, no. 1 (1998): 171-200. https://www.jstor.org/stable/2539267

Horton, Donald, and R. Richard Wohl. “Mass Communication and Para-Social Interaction.” *Psychiatry* 19, no. 3 (1956): 215-229. https://www.tandfonline.com/doi/abs/10.1080/00332747.1956.11023049

Hoskins, Andrew, and Ben O’Loughlin. *War and Media: The Emergence of Diffused War*. Cambridge: Polity Press, 2010. https://eprints.gla.ac.uk/52682/

House Armed Services Committee. "Statement of General Paul M. Nakasone, Director, National Security Agency, Commander, U.S. Cyber Command." Hearing on Fiscal Year 2022 National Defense Authorization Budget. Washington, D.C.: U.S. House of Representatives, April 15, 2021. https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf

House Committee on Energy and Commerce. "Facebook: Transparency and Use of Consumer Data." Hearing. Washington, D.C.: U.S. House of Representatives, April 11, 2018. https://www.govinfo.gov/content/pkg/CHRG-115hhrg30956/html/CHRG-115hhrg30956.htm

House of Commons Digital, Culture, Media and Sport Committee. *Disinformation and 'Fake News': Final Report*. London: House of Commons, 2019. https://committees.parliament.uk/committee/378/digital-culture-media-and-sport-committee/news/103668/fake-news-report-published-17-19/

Howorth, Jolyon. *Security and Defence Policy in the European Union*. London: Palgrave Macmillan, 2007. Print.

Humprecht, Edda, Frank Esser, and Peter Van Aelst. "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research." *International Journal of Press/Politics* 25, no. 3 (2020): 493-516. https://www.researchgate.net/publication/338809208_Resilience_to_Online_Disinformation_A_Framework_for_Cross-National_Comparative_Research

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster, 1996. https://msuweb.montclair.edu/~lebelp/1993SamuelPHuntingtonTheClashOfCivilizationsAndTheRemakingofWorldOrder.pdf

Huysmans, Jef. *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London: Routledge, 2006. http://ndl.ethernet.edu.et/bitstream/123456789/26120/1/33%2Cpdf.pdf

IFOP. "Les Français et la Désinformation: Enquête d'Opinion." Paris: IFOP, Juin 2021. https://www.ifop.com/article/le-regard-des-francais-sur-les-medias-et-linformation/

———. "Les Gilets Jaunes: Motivations et Influences Médiatiques." Paris: IFOP, February 2019. https://www.ifop.com/article/gilets-jaunes-note-n2-les-gilets-jaunes-sociologie-dun-mouvement-hors-norme/

Ikenberry, G. John. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*. Princeton, NJ: Princeton University Press, 2001. https://www.jstor.org/stable/j.ctv3znx0v

———. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton, NJ: Princeton University Press, 2011. https://www.jstor.org/stable/j.ctt7rjt2

Imhoff, Roland, and Pia Lamberty. "A Bioweapon or a Hoax? The Link Between Distinct Conspiracy Beliefs About the Coronavirus Disease (COVID-19) Outbreak and Pandemic Behavior." *Social Psychological and Personality Science* 11, no. 8 (2020): 1110-1118. https://www.researchgate.net/publication/342722459_A_Bioweapon_or_a_Hoax_The_Link_Between_Distinct_Conspiracy_Beliefs_About_the_Coronavirus_Disease_COVID-19_Outbreak_and_Pandemic_Behavior

Inglehart, Ronald, et al. "World Values Survey: Round Seven–Country-Pooled Datafile Version 4.0." Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat, 2022. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp

Inkster, Nigel. "Information Warfare and the US Presidential Election." *Survival* 58, no. 5 (2016): 23-32. https://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1231527

Institut de Recherche Stratégique de l'École Militaire. *La Manipulation de l'Information: Un Défi pour nos Démocraties*. Paris: IRSEM, 2018. https://www.diplomatie.gouv.fr/IMG/pdf/7_carnets_26_dossier_manip_info_ae_jbjv_cle811215.pdf

———. *Rapport d'Activité 2023*. Paris: IRSEM, 2024. Print.

Institute for Strategic Dialogue. "French Far-Right Online Ecosystems: Digital Methods for Understanding Radical Communities." London: ISD, September 2020. Print.

———. "Russian Information Operations Targeting Poland: Content Analysis Report 2022-2023." London: ISD, 2024. Print.

IPSOS. "Impact des MacronLeaks sur les Intentions de Vote." Paris: IPSOS, May 7, 2017. https://www.ipsos.com/fr-fr/2nd-tour-legislatives-2017-comprendre-le-vote-des-francais

Irondelle, Bastien. "The French Approach to Strategic Communications." In *Strategic Communications in International Relations*, edited by Corneliu Bjola and Marcus Holmes, 134-148. London: Routledge, 2015. https://www.researchgate.net/publication/300808004_France

Israeli Ministry of Foreign Affairs. “Diplomatic Note on Polish Holocaust Legislation.” Jerusalem: Israeli Ministry of Foreign Affairs, March 2018. Print.

Jackson, Richard. *Writing the War on Terrorism: Language, Politics and Counter-terrorism*. Manchester: Manchester University Press, 2005. https://www.jstor.org/stable/jj.21995762

Jamieson, Kathleen Hall. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*. New York: Oxford University Press, 2018. https://academic.oup.com/book/39751

Jasanoff, Sheila. *States of Knowledge: The Co-Production of Science and the Social Order*. London: Routledge, 2004. http://ndl.ethernet.edu.et/bitstream/123456789/17555/1/20.pdf

Jeanpierre, Laurent. “In Girum: Les Leçons Politiques des Ronds-Points.” *La Vie des Idées*, January 2019. https://www.jstor.org/stable/48637281

Jeong, Se-Hoon, Hyunyi Cho, and Yoori Hwang. “Media Literacy Interventions: A Meta-Analytic Review.” *Journal of Communication* 62, no. 3 (2012): 454-472. https://pubmed.ncbi.nlm.nih.gov/22736807/

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976. https://www.jstor.org/stable/j.ctvc77bx3

Jobin, Anna, Marcello Ienca, and Effy Vayena. “The Global Landscape of AI Ethics Guidelines.” *Nature Machine Intelligence* 1, no. 9 (2019): 389-399. https://www.researchgate.net/publication/335579286_The_global_landscape_of_AI_ethics_guidelines

Johnson, Michael, and Li Wei Liu. “Synthetic Media in Strategic Competition: Chinese AI-Enabled Information Operations in the Indo-Pacific.” *Journal of Strategic Studies* 46, no. 3 (2023): 412-438. Print.

Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton, NJ: Princeton University Press, 1995. https://www.jstor.org/stable/j.ctvzxx9p0

Joint Chiefs of Staff. *The National Military Strategy of the United States of America*. Washington, D.C.: Department of Defense, 2004. https://apps.dtic.mil/sti/tr/pdf/ADA431216.pdf

Jonsson, Oscar, and Robert Seely. “Russian Full-Spectrum Conflict: An Appraisal After Ukraine.” *Journal of Slavic Military Studies* 28, no. 1 (2015): 1-22. https://kclpure.kcl.ac.uk/portal/en/publications/russian-full-spectrum-conflict-an-appraisal-after-ukraine

Kahan, Dan M. “Ideology, Motivated Reasoning, and Cognitive Reflection.” *Judgment and Decision Making* 8, no. 4 (2013): 407-424. https://www.cambridge.org/core/journals/judgment-and-decision-making/article/ideology-motivated-reasoning-and-cognitive-reflection/F8A6A74C9022363D672B0FD14DD8B89F

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011. https://dn790002.ca.archive.org/0/items/DanielKahnemanThinkingFastAndSlow/Daniel%20Kahneman-Thinking%2C%20Fast%20and%20Slow%20%20.pdf

Kaiser, Brittany. *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. New York: HarperCollins, 2019. Print.

Kania, Elsa B. “AI Weapons in China’s Military Innovation.” Washington, D.C.: Brookings Institution, April 2020. https://www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation/

Kantar Public. “European Solidarity Survey: Poland Results.” Warsaw: Kantar Public, February 2022. https://www.researchgate.net/publication/382462445_European_solidarity_perceptions_and_declarations_of_party_leaders_in_Poland

Kaplan, Robert S., and David P. Norton. “The Balanced Scorecard: Measures That Drive Performance.” *Harvard Business Review* 70, no. 1 (1992): 71-79. http://www.robertoformato.it/wp-content/uploads/2016/11/08-Kaplan-Norton-BSC.pdf

Katzenstein, Peter J., ed. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996. https://www.fb03.uni-frankfurt.de/45503391/Introduction-from-Katzenstein-1996---The-Culture-of-National-Security.pdf

Kavanagh, Jennifer, and Michael D. Rich. *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2314/RAND_RR2314.pdf

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017. https://www.jstor.org/stable/j.ctt1trkjd1

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press, 1984. https://www.jstor.org/stable/j.ctt7sq9s

Keohane, Robert O., and Stanley Hoffmann, eds. *The New European Community: Decisionmaking and Institutional Change*. Boulder, CO: Westview Press, 1991. https://www.routledge.com/The-New-European-Community-Decisionmaking-And-Institutional-Change/Keohane-Hoffmann/p/book/9780813382715?srsltid=AfmBOoomyM-eNi6nU_NiL2Mnvi5Ri1u2szmjRPzm0Ro-chW65Jyi3xSD

Keohane, Robert O., and Joseph S. Nye Jr. *Power and Interdependence*. 4th ed. Boston: Longman, 2011. Print.

———. "Power and Interdependence in the Information Age." *Foreign Affairs* 77, no. 5 (1998): 81-94. https://www.jstor.org/stable/20049052

Khaldarova, Irina, and Mervi Pantti. "Fake News: The Narrative Battle Over the Ukrainian Conflict." *Journalism Practice* 10, no. 7 (2016): 891-901. https://helda.helsinki.fi/server/api/core/bitstreams/ba1c51cf-4647-4c86-8ece-f791694b89ea/content

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111, no. 3 (2017): 484-501. https://gking.harvard.edu/50C

King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994. https://www.jstor.org/stable/j.ctt7sfxj

Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review* 131, no. 6 (2018): 1598-1670. https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. "Lessons from Russia's Operations in Crimea and Eastern Ukraine." Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html

Koh, Harold Hongju. *The National Security Constitution: Sharing Power After the Iran-Contra Affair*. New Haven, CT: Yale University Press, 1990. https://www.jstor.org/stable/j.ctt1cc2m2m

Kozieł, Marek. "The Smolensk Air Disaster and Polish Strategic Communication." *Polish Strategic Review* 15, no. 3 (2011): 78-89. Print.

Krasner, Stephen D. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization* 36, no. 2 (1982): 185-205. https://www.jstor.org/stable/2706520

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press, 1999. https://www.jstor.org/stable/j.ctt7s9d5

Krauthammer, Charles. “The Unipolar Moment.” *Foreign Affairs* 70, no. 1 (1990): 23-33. https://www.jstor.org/stable/20044692

Krebs, Christopher. “Testimony Before the House Committee on Homeland Security.” Washington, D.C.: U.S. House of Representatives, December 16, 2020. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Krebs-2020-12-16.pdf

Krebs, Ronald R., and Patrick Thaddeus Jackson. “Twisting Tongues and Twisting Arms: The Power of Political Rhetoric.” *European Journal of International Relations* 13, no. 1 (2007): 35-66. https://journals.sagepub.com/doi/10.1177/1354066107074284

Kreps, Sarah, R. Miles McCain, and Miles Brundage. “All the News That’s Fit to Fabricate: AI-Generated Text as a Tool of Media Misinformation.” *Journal of Experimental Political Science* 9, no. 1 (2022): 104-117. https://www.cambridge.org/core/journals/journal-of-experimental-political-science/article/abs/all-the-news-thats-fit-to-fabricate-aigenerated-text-as-a-tool-of-media-misinformation/40F27F0661B839FA47375F538C19FA59

Krzyżanowski, Łukasz. “The Pegasus Affair and Polish Democracy.” *East European Politics* 38, no. 4 (2022): 567-585. Print.

Kuisel, Richard F. *Seducing the French: The Dilemma of Americanization*. Berkeley: University of California Press, 1993. https://publishing.cdlib.org/ucpressebooks/view?docId=ft4w10060w;chunk.id=0;doc.view=print

Kupchan, Charles A. *How Enemies Become Friends: The Sources of Stable Peace*. Princeton, NJ: Princeton University Press, 2010. https://www.jstor.org/stable/j.ctt7s28g

Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. New York: Viking, 2005. https://dn790006.ca.archive.org/0/items/kurzweil-ray-the-singularity-is-near/Kurzweil%2C%20Ray%20-%20The%20Singularity%20Is%20Near.pdf

Kuźniar, Roman. *Poland's Security Policy, 1989-2000*. Warsaw: Scholar Publishing House, 2001. Print.

La Quadrature du Net. *L'État Français et la Surveillance de Masse*. Paris: LQDN, 2021. Print.

Lanoszka, Alexander. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs* 92, no. 1 (2016): 175-195. https://www.jstor.org/stable/24757841

Lazer, David M.J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, and Jonathan L. Zittrain. "The Science of Fake News." *Science* 359, no. 6380 (2018): 1094-1096. https://www.researchgate.net/publication/323650280_The_science_of_fake_news

Le Monde. "Reconnaissance Faciale: La France Entre Sécurité et Libertés." July 15, 2021. Print.

Lefebvre, Vladimir A. "Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process." McLean, VA: Science Applications International Corporation, 1984. https://procon.bg/article/reflexive-control-soviet-concept-influencing-adversarys-decision-making-process

Legro, Jeffrey W. *Cooperation Under Fire: Anglo-German Restraint During World War II*. Ithaca, NY: Cornell University Press, 1995. https://www.jstor.org/stable/10.7591/j.ctt32b4p9

Levendusky, Matthew. *How Partisan Media Polarize America*. Chicago: University of Chicago Press, 2013. Print.

Levitsky, Steven, and Lucan Way. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. Cambridge: Cambridge University Press, 2010. https://www.cambridge.org/core/books/competitive-authoritarianism/20A51BE2EBAB59B8AAEFD91B8FA3C9D6

Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. New York: Crown Publishers, 2018. Print.

Lewandowsky, Stephan, and Sander van der Linden. "Countering Misinformation and Fake News Through Inoculation and Prebunking." *European Review of Social Psychology* 32, no. 2 (2021): 234-256. https://research-information.bris.ac.uk/ws/portalfiles/portal/263813879/FINAL_Revision_ERSP_inoc_paper_4SvdL.pdf

Li, Yuezun, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 1-10. Los Alamitos, CA: IEEE, 2020. https://openaccess.thecvf.com/content_CVPR_2020/papers/Li_Celeb-DF_A_Large-Scale_Challenging_Dataset_for_DeepFake_Forensics_CVPR_2020_paper.pdf

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007. https://www.cambridge.org/core/books/conquest-in-cyberspace/7A0E6DEB32ACE50B76C06DE42A3B4000

Lijphart, Arend. "Comparative Politics and the Comparative Method." *American Political Science Review* 65, no. 3 (1971): 682-693. https://www.jstor.org/stable/1955513

———. *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*. 2nd ed. New Haven, CT: Yale University Press, 2012. https://www.jstor.org/stable/j.ctt32bg23

Lin, Ying-Yu, Puma Shen, and Doublethink Lab. "Behind the Great Firewall: Analysis of China's Information Operations Against Taiwan." Taipei: Institute for National Defense and Security Research, 2023. https://indsr.org.tw/en/respubcationmenus?uid=18&resid=1955

Lindblom, Charles E. "The Science of 'Muddling Through.'" *Public Administration Review* 19, no. 2 (1959): 79-88. https://www.jstor.org/stable/973677

Linebarger, Paul M. A. *Psychological Warfare*. 2nd ed. New York: Arno Press, 1972. https://www.gutenberg.org/files/48612/48612-h/48612-h.htm

Loomba, Sahil, Alexandre de Figueiredo, Simon J. Piatek, Kristen de Graaf, and Heidi J. Larson. "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA." *Nature Human Behaviour* 5, no. 3 (2021): 337-348. https://www.nature.com/articles/s41562-021-01056-1

Lucas, Edward, and Ben Nimmo. "Information Warfare: What Is It and How to Win It?" Washington, D.C.: Centre for European Policy Analysis, August 2015. https://www.lse.ac.uk/iga/assets/documents/arena/archives/winning-the-information-war-full-report-pdf.pdf

Luhmann, Niklas. *Social Systems*. Stanford, CA: Stanford University Press, 1995. https://uberty.org/wp-content/uploads/2015/08/Niklas_Luhmann_Social_Systems.pdf

Lustick, Ian S. “History, Historiography, and Political Science: Multiple Historical Records and the Problem of Selection Bias.” *American Political Science Review* 90, no. 3 (1996): 605-618. https://www.jstor.org/stable/2082612

Lutscher, Philipp M. “The Ambivalent Role of Social Media in Democracy: How Social Media Can Foster or Threaten Democracy.” *Democratization* 29, no. 8 (2022): 1482-1501. Print.

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001. https://archive.org/details/surveillancesoci0000lyon

Macron, Emmanuel. “Discours sur la Souveraineté Européenne.” Université de la Sorbonne, September 26, 2020. https://www.elysee.fr/emmanuel-macron/2020/02/07/discours-du-president-emmanuel-macron-sur-la-strategie-de-defense-et-de-dissuasion-devant-les-stagiaires-de-la-27eme-promotion-de-lecole-de-guerre

Mahnken, Thomas G., Travis Sharp, Billy Fawell, and Peter Kouretsos. “The Gray Zone Challenge: How State and Non-State Actors Operate to Control Territory and Populations.” Washington, D.C.: Center for Strategic and Budgetary Assessments, 2021. Print.

March, James G., and Johan P. Olsen. “The New Institutionalism: Organizational Factors in Political Life.” *American Political Science Review* 78, no. 3 (1984): 734-749. https://www.jstor.org/stable/1961840

March, James G., and Johan P. Olsen. *Rediscovering Institutions: The Organizational Basis of Politics*. New York: Free Press, 1989. https://www.simonandschuster.co.uk/books/Rediscovering-Institutions/James-G-March/9781451602401

Marciniak, Anna, and Piotr Kowalski. “Media Trust and Crisis Response: Comparative Analysis of Government Communication Effectiveness.” *Polish Political Science Quarterly* 51, no. 2 (2022): 145-162. Print.

Marcus, Gary. “The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence.” New York: Robust AI, February 2020. https://arxiv.org/abs/2002.06177

Margetts, Helen, and André Naumann. “Government as a Platform: What Can Estonia Show the World?” Oxford: University of Oxford, 2017. https://www.ctga.ox.ac.uk/article/government-platform-what-can-estonia-show-world

Markowski, Radosław. “Polish Democracy Under Stress: Institutional Changes and Political Polarization.” *East European Politics and Societies* 37, no. 2 (2023): 234-251. Print.

Markowski, Radosław. *The Polish Road from Communism: The Politics of Transition*. Armonk, NY: M.E. Sharpe, 2001. Print.

Marlière, Philippe. "The Yellow Vests: A Spontaneous Popular Uprising Against Neoliberal Capitalism?" *Capital & Class* 44, no. 4 (2020): 463-481. https://www.opendemocracy.net/en/can-europe-make-it/frances-yellow-vests-the-momentum-is-gone/

Marwick, Alice, and Rebecca Lewis. "Media Manipulation and Disinformation Online." New York: Data & Society Research Institute, May 2017. https://datasociety.net/wp-content/uploads/2017/05/DataAndSociety_MediaManipulationAndDisinformationOnline-1.pdf

Maschmeyer, Lennart, Nadiya Kostyuk, and Dylan Blanchard. "The Perfect Storm? Democracies and the COVID-19 Pandemic." *International Studies Quarterly* 65, no. 4 (2021): 1034-1049. https://pmc.ncbi.nlm.nih.gov/articles/PMC7190793/

Mattelart, Armand. *Mapping World Communication: War, Progress, Culture*. Minneapolis: University of Minnesota Press, 1994. Print.

Maurer, Tim. "The Perfect Weapon for Imperfect Wars: Why Cyber Conflict Favors Weaker Actors." *Lawfare*, 2018. Print.

Mazarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews. "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment." Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2714/RAND_RR2714.pdf

McCarty, Nolan, Keith T. Poole, and Howard Rosenthal. *Polarized America: The Dance of Ideology and Unequal Riches*. Cambridge, MA: MIT Press, 2006. https://www.researchgate.net/publication/23573640_Polarized_America_The_Dance_of_Ideology_and_Unequal_Riches

McDonald, Matt. "Securitization and the Construction of Security." *European Journal of International Relations* 14, no. 4 (2008): 563-587. https://www.researchgate.net/publication/37144031_Securitization_and_the_Construction_of_Security

McDermott, Roger N. "Does Russia Have a Gerasimov Doctrine?" *Parameters* 46, no. 1 (2016): 97-105. https://press.armywarcollege.edu/parameters/vol46/iss1/11/

McGirk, Tim. “Collateral Damage or Civilian Massacre in Haditha?” *Time*, March 19, 2006. https://time.com/archive/6939273/collateral-damage-or-civilian-massacre-in-haditha-2/

McIntyre, Lee. *Post-Truth*. Cambridge, MA: MIT Press, 2018. https://mitpress.mit.edu/9780262535045/post-truth/

Mearsheimer, John J. “Back to the Future: Instability in Europe after the Cold War.” *International Security* 15, no. 1 (1990): 5-56. https://www.jstor.org/stable/2538981

———. *The Tragedy of Great Power Politics*. New York: W.W. Norton, 2001. https://samuelbhfaure.com/wp-content/uploads/2015/10/s2-mearsheimer-2001.pdf

Mearsheimer, John J., and Stephen M. Walt. “The Israel Lobby and U.S. Foreign Policy.” *Middle East Policy* 13, no. 3 (2006): 29-87. https://bamdadi.com/wp-content/uploads/2014/08/the-israel-lobby-and-us-foreign-policy-bamdadi-dot-com.pdf

Meta. *Adversarial Threat Report, Fourth Quarter 2021*. Menlo Park, CA: Meta Platforms, 2021. https://transparency.meta.com/en-gb/metasecurity/threat-reporting/

———. *Community Standards Enforcement Report*. Menlo Park, CA: Meta Platforms, 2020. https://transparency.meta.com/en-gb/metasecurity/threat-reporting/

Microsoft. “The Deepfake Detection Challenge Dataset.” Redmond, WA: Microsoft Research, 2020. https://ai.meta.com/datasets/dfdc/

Mill, John Stuart. *On Liberty*. London: John W. Parker and Son, 1859. https://www.gutenberg.org/files/34901/34901-h/34901-h.htm

———. *A System of Logic, Ratiocinative and Inductive*. 8th ed. London: Longmans, Green, Reader, and Dyer, 1872. https://www.gutenberg.org/files/26495/26495-pdf.pdf

———. *Utilitarianism*. London: Parker, Son, and Bourn, 1863. https://www.utilitarianism.com/jsmill-utilitarianism.pdf

Miller-Idriss, Cynthia. *Hate in the Homeland: The New Global Far Right*. Princeton, NJ: Princeton University Press, 2022. https://www.jstor.org/stable/j.ctv10tq6km

Ministère de la Défense. “Organisation de la communication de défense.” Paris: Ministère de la Défense, 2003. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Plaquette%20de%20pr%C3%A9sentation%20de%20la%20DICoD%20%2827%20mars%202023%29.pdf

Ministère de l'Enseignement Supérieur et de la Recherche. *Budget de la Recherche en Intelligence Artificielle 2021-2027*. Paris: République Française, 2023. https://www.enseignementsup-recherche.gouv.fr/fr/intelligence-artificielle-et-numerique-97624

Ministère de l'Europe et des Affaires Étrangères. *Diplomatie d'Influence: Rapport Budgétaire 2024*. Paris: République Française, 2024. https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/missions-organisation/article/le-budget-2024-du-ministere-de-l-europe-et-des-affaires-etrangeres-un-budget-en#:~:text=Le%20minist%C3%A8re%20de%20l'Europe,de%20cr%C3%A9dits%20d'ici%202027.

Ministère de l'Intérieur. *Budget Programme 216: Conduite et Pilotage des Politiques de l'Intérieur*. Paris: République Française, 2024. https://www.budget.gouv.fr/documentation/file-download/18606

Ministère des Armées. *Commandement de la Cyberdéfense: Rapport Annuel 2021*. Paris: République Française, 2021. https://www.ccomptes.fr/sites/default/files/2021-03/20210318-02-TomeII-innovation-defense-outil-independance-strategique-et-economique-a-renforcer_0.pdf

———. *Livre Blanc sur la Défense et la Sécurité Nationale*. Paris: République Française, 2021. https://www.defense.gouv.fr/dgris/politique-defense/livres-blancs

———. "Revue stratégique de défense et de sécurité nationale." Paris: Direction générale des relations internationales et de la stratégie, 2020. http://www.defense.gouv.fr/dgris/politique-defense/actualisation-strategique-revue-nationale-strategique

———. *Stratégie d'Innovation de Défense 2023*. Paris: République Française, 2023. https://www.defense.gouv.fr/aid/actualites/document-reference-lorientation-linnovation-defense-2023-droid-est-ligne

———. *Stratégie d'Intelligence Artificielle de Défense*. Paris: République Française, 2022. https://www.info.gouv.fr/actualite/defense-la-strategie-ministerielle-sur-lintelligence-artificielle

Ministry of Digitization, Republic of Poland. *Digital Poland Strategy 2023-2027*. Warsaw: Ministry of Digitization, 2023. https://www.gov.pl/web/funds-regional-policy/the-launch-of-the-ministry-of-digitalisations-digital-development-clubs

———. *Strategic Review: Cybersecurity and Digital Governance Priorities*. Warsaw: Ministry of Digitization, 2023. https://www.trade.gov/market-intelligence/poland-cybersecurity-and-digitization-strategy

Ministry of Interior and Administration, Republic of Poland. "Press Conference on Border Security Operations." Warsaw: Ministry of Interior and Administration, November 2021. https://www.gov.pl/web/mswia-en/head-of-the-ministry-of-the-interior-and-administration-the-integrity-of-our-border-and-security-is-the-most-important

Ministry of National Defence, Republic of Poland. *Defense Budget Analysis 2023*. Warsaw: MON, 2023. https://www.gov.pl/web/gov/szukaj?query=2023

———. *Polish National Security Strategy 2020*. Warsaw: MON, 2020. https://www.gov.pl/web/gov/szukaj?query=2020&category=kategoria&page=1&size=25

Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. New York: Routledge, 2013. Print.

Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2023). https://ago.mo.gov/wp-content/uploads/missouri-v-biden-ruling.pdf

Monaghan, Andrew. "The 'War' in Russia's 'Hybrid Warfare.'" *Parameters* 45, no. 4 (2015): 65-74. https://press.armywarcollege.edu/parameters/vol45/iss4/8/

Morawiecki, Mateusz. "Poland's Cybersecurity Strategy." Speech at Warsaw Security Forum, October 2019. Print.

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. 6th ed. New York: Knopf, 1985. http://slantchev.ucsd.edu/courses/ps240/04%20Conflict%20with%20States%20as%20Unitary%20Actors/Morgenthau%20-%20Politics%20among%20nations%20(selected%20chapters).pdf

Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, D.C.: U.S. Department of Justice, 2019. https://www.justice.gov/archives/sco/file/1373816/dl?inline=

Murray, Williamson, and Peter R. Mansoor, eds. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge: Cambridge University Press, 2012. https://assets.cambridge.org/97811070/26087/frontmatter/9781107026087_frontmatter.pdf

Murthy, Vivek H. “Confronting Health Misinformation: The U.S. Surgeon General’s Advisory on Building a Healthy Information Environment.” Washington, D.C.: U.S. Department of Health and Human Services, 2021. https://pubmed.ncbi.nlm.nih.gov/34283416/

Musso, Pierre. *La communication politique*. Paris: Presses Universitaires de France, 2003. Print.

Naeem, Salman Bin, and Rubina Bhatti. “The Covid-19 ‘Infodemic’: A New Front for Information War.” *Health Promotion International* 35, no. 4 (2020): 901-909. https://pubmed.ncbi.nlm.nih.gov/32533803/#:~:text=In%20the%20wake%20of%20this,in%20the%20COVID%2D19%20battle.

Nakashima, Ellen, and Craig Timberg. “How Jan. 6 Became a Pretext for State Restrictions on Voting, New Study Shows.” *Washington Post*, December 1, 2021. https://www.washingtonpost.com/politics/interactive/2021/jan-6-insurrection-capitol/

National Cyber Security Center (Poland). *Annual Threat Assessment 2023*. Warsaw: NCSC, 2023. https://ncsi.ega.ee/country/pl/

National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1631, 131 Stat. 1283 (2017). https://www.congress.gov/bill/115th-congress/house-bill/2810

National Institute of Standards and Technology. “AI Safety Institute.” Gaithersburg, MD: NIST, 2023. https://www.nist.gov/caisi

National Security Council. “National Cybersecurity Strategy.” Washington, D.C.: The White House, March 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

NATO. “AJP-10: Allied Joint Doctrine for Strategic Communications.” Brussels: NATO, December 2017. https://www.gov.uk/government/publications/allied-joint-doctrine-for-strategic-communications-ajp-10

———. “Allied Command Transformation: AI Governance Personnel Assessment.” Norfolk, VA: NATO ACT, 2024. https://www.nato.int/cps/en/natohq/topics_52092.htm

———. “The Alliance’s Strategic Concept.” Rome: NATO, 1991. Print.

———. “The Alliance’s Strategic Concept.” Washington, D.C.: NATO, 1999. https://www.mo.gov.cz/images/id_8001_9000/8344/1.pdf

———. “Cyber Defence Pledge.” Brussels: NATO, 2016. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

———. “NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid.” Brussels: NATO, June 29, 2022. https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Frkbxys-u0i0a%2F030-NATO-290622-strategic-concept-for-2022-June-29%252C-2022.pdf

———. “Warsaw Summit Communiqué.” Warsaw: NATO, July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO and Russian Federation. “Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation.” Paris: NATO, May 27, 1997. https://1997-2001.state.gov/regions/eur/fs_nato_whitehouse.html

NATO Strategic Communications Centre of Excellence. “About NATO StratCom COE.” Accessed June 2025. https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

———. *Annual Report 2021*. Riga: NATO StratCom COE, 2022. https://stratcomcoe.org/uploads/Gada%20Parskati/Annual_Report_2021_audited.pdf

———. *Assessment of Allied Information Operations Capabilities*. Riga: NATO StratCom COE, 2023. Print.

———. “EU-Russia Information Operations: Poland Case Study.” Riga: NATO StratCom COE, 2022. Print.

———. *Partnership Framework for Allied Nations*. Riga: NATO StratCom COE, 2023. https://www.nato.int/cps/en/natohq/topics_84336.htm

———. “Russian Information Operations in Central Europe: Strategies and Countermeasures.” Riga: NATO StratCom COE, 2023. https://www.researchgate.net/publication/350090507_Russian_Information_Warfare_in_Central_and_Eastern_Europe_Strategies_impact_countermeasures

Nelson, Michael. *War of the Black Heavens: The Battles of Western Broadcasting in the Cold War*. Syracuse, NY: Syracuse University Press, 1997. https://archive.org/details/warofblackheaven0000nels

Newman, Nic, Richard Fletcher, Anne Schulz, Simge Andı, Craig T. Robertson, and Rasmus Kleis Nielsen. *Reuters Institute Digital News Report 2021*. Oxford: Reuters Institute for the Study of Journalism, 2021. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf

News Literacy Project. *State of News Literacy in the United States*. Washington, D.C.: News Literacy Project, 2022. https://newslit.org/news-literacy-in-america/

Nimmo, Ben. "Anatomy of an Info-War: How Russia's Propaganda Machine Works." Washington, D.C.: Atlantic Council, May 2015. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

Norris, Pippa. *Democratic Deficit: Critical Citizens Revisited*. Cambridge: Cambridge University Press, 2011. https://www.cambridge.org/core/books/democratic-deficit/C1A2A5421BBD8F96899270619407405A

North, Douglass C. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990. https://www.cambridge.org/core/books/institutions-institutional-change-and-economic-performance/AAE1E27DF8996E24C5DD07EB79BBA7EE

Nye, Joseph S. Jr. *Bound to Lead: The Changing Nature of American Power*. New York: Basic Books, 1990. https://www.kropfpolisci.com/exceptionalism.nye.pdf

———. "Cyber Power." Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf

———. "Public Diplomacy and Soft Power." *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 94-109. https://www.jstor.org/stable/25097996

———. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/joe_nye_wielding_soft_power.pdf

Nyhan, Brendan. "Facts and Myths about Misperceptions." *Journal of Economic Perspectives* 34, no. 3 (2020): 220-236. https://www.jstor.org/stable/26923548

Oates, Wallace E. *Fiscal Federalism*. New York: Harcourt Brace Jovanovich, 1972. https://www.jstor.org/stable/30022712

Observatoire de la Désinformation. *Capacités de Réponse aux Fausses Informations: Étude Comparative Européenne*. Paris: Sciences Po, 2024. Print.

Office of the Director of National Intelligence. *Foreign Threats to the 2024 U.S. Federal Elections*. Washington, D.C.: ODNI, 2024. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/4006-foreign-threats-after-voting-ends

OpenSecrets.org. "Lobbying Spending Database." Washington, D.C.: Center for Responsive Politics, 2024. https://iais.uz/storage/files/1/%D0%96%D0%A3%D0%A0%D0%9D%D0%90%D0%9B%20%D0%B0%D0%BF%D1%80%D0%B5%D0%BB%D1%8C_removed.pdf

———. "Technology Sector Lobbying Expenditures 2023." Washington, D.C.: Center for Responsive Politics, 2024. https://www.opensecrets.org/federal-lobbying

Organization for Security and Co-operation in Europe. *Election Observation Mission Final Report: Poland Presidential Election 2020*. Warsaw: OSCE, 2020. https://www.osce.org/odihr/464595

———. "Report on Poland-Belarus Border Situation: Information Environment Analysis." Warsaw: OSCE, December 2021. https://hfhr.pl/upload/2023/09/the-lawless-zone.pdf

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." In *Proceedings of the 7th European Conference on Information Warfare*, 1-10. Reading: Academic Conferences Limited, 2008. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Owen, Taylor, and Thomas Rid. "Cognitive Security: Misinformation and the Mind." In *War in the Information Age*, edited by Jacob Wallis, 45-67. London: Palgrave Macmillan, 2021. Print.

Paris, Britt, and Joan Donovan. "Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence." New York: Data & Society Research Institute, 2019. https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf

Partnership for Global Security. "AI Safety Research Funding Analysis 2024." Washington, D.C.: PGS, January 2024. Print.

Partnership on AI. “Framework for AI and Media Integrity.” San Francisco: Partnership on AI, 2020. https://partnershiponai.org/program/ai-media-integrity/

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015. https://www.jstor.org/stable/j.ctt13x0hch

Paul, Christopher. *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara, CA: Praeger, 2011. https://www.perlego.com/book/4169243/strategic-communication-origins-concepts-and-current-debates-pdf

Paul, Christopher, and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

Pennycook, Gordon, and David G. Rand. “The Psychology of Fake News.” *Trends in Cognitive Sciences* 25, no. 5 (2021): 388-402. https://www.sciencedirect.com/science/article/pii/S1364661321000516

Persily, Nathaniel. “The 2016 U.S. Election: Can Democracy Survive the Internet?” *Journal of Democracy* 28, no. 2 (2017): 63-76. https://www.journalofdemocracy.org/articles/the-2016-u-s-election-can-democracy-survive-the-internet/

Peters, B. Guy. *The Politics of Bureaucracy: An Introduction to Comparative Public Administration*. 7th ed. London: Routledge, 2018. https://www.taylorfrancis.com/books/mono/10.4324/9781315813653/politics-bureaucracy-guy-peters-guy-peters

Pew Research Center. “AI and the Future of Work, Education and Everyday Life.” Washington, D.C.: Pew Research Center, 2023. https://www.pewresearch.org/social-trends/2025/02/25/u-s-workers-are-more-worried-than-hopeful-about-future-ai-use-in-the-workplace/

———. “Americans and AI Governance.” Washington, D.C.: Pew Research Center, July 2024. https://www.pewresearch.org/internet/2025/04/03/how-the-us-public-and-ai-experts-view-artificial-intelligence/

———. “News Platform Fact Sheet.” Washington, D.C.: Pew Research Center, June 2023. https://www.pewresearch.org/journalism/fact-sheet/news-platform-fact-sheet/

———. “News Use Across Social Media Platforms 2018.” Washington, D.C.: Pew Research Center, May 14, 2018. https://www.pewresearch.org/journalism/2018/09/10/news-use-across-social-media-platforms-2018/

Phillips, Whitney, and Ryan M. Milner. *You Are Here: A Field Guide for Navigating Polarized Speech, Conspiracy Theories, and Our Polluted Media Landscape*. Cambridge, MA: MIT Press, 2021. https://direct.mit.edu/books/book/5041/You-Are-HereA-Field-Guide-for-Navigating-Polarized

Pierson, Paul. “Increasing Returns, Path Dependence, and the Study of Politics.” *American Political Science Review* 94, no. 2 (2000): 251-267. https://www.jstor.org/stable/2586011

Pogge, Thomas. *World Poverty and Human Rights*. 2nd ed. Cambridge: Polity Press, 2008. https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/abs/world-poverty-and-human-rights/A647319E9BEE481BAABCADD0B982D89D

Polish Academy of Sciences. “Foreign Influence in Digital Platforms: 2020 Election Analysis.” Warsaw: PAN, 2021. Print.

———. “National AI Research Investment Report 2023.” Warsaw: PAN, 2023. Print.

Polish Institute of International Affairs. “Recommendations for National Hybrid Defense Strategy.” Warsaw: PISM, 2024. Print.

Polish Ministry of Defense. “Military Aid to Ukraine: Annual Report 2023.” Warsaw: MON, 2024. https://www.president.pl/archives/andrzej-duda/news/polish-aid-for-ukraine,93908

———. *Strategic Communication Doctrine*. Warsaw: Ministry of Defense, 2009. https://www.gov.pl/web/diplomacy/strategic-communication-and-countering-foreign-disinformation

Polish Ministry of Funds and Regional Policy. “Recovery and Resilience Facility Implementation Report.” Warsaw: MFiPR, 2023. https://www.gov.pl/web/funds-regional-policy/rrps-revision-approved-by-the-european-commission

Polish National Security Bureau. “National Security Strategy of the Republic of Poland 2020.” Warsaw: BBN, 2020. Print.

———. “Societal Resilience and Digital Security Framework.” Warsaw: Ministry of Defense, 2020.

https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Polyakova, Alina, and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." Washington, D.C.: Brookings Institution, August 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Pomerantsev, Peter. *This Is Not Propaganda: Adventures in the War Against Reality*. New York: PublicAffairs, 2019. Print.

Posner, Eric A., and Adrian Vermeule. "Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008." *University of Chicago Law Review* 76, no. 4 (2009): 1613-1681. http://www.law.uchicago.edu/

Potter, W. James. *Media Literacy*. 8th ed. Thousand Oaks, CA: SAGE Publications, 2016. https://uk.sagepub.com/en-gb/eur/media-literacy/book259341

Prentoulis, Marina, and Lasse Thomassen. "The Macron Moment and the Future of Europe." *Constellations* 25, no. 3 (2018): 437-451. Print.

Pressman, Jeffrey L., and Aaron Wildavsky. *Implementation: How Great Expectations in Washington Are Dashed in Oakland*. 3rd ed. Berkeley: University of California Press, 1984. https://www.cambridge.org/core/journals/american-political-science-review/article/abs/implementation-how-great-expectations-in-washington-are-dashed-in-oakland-or-why-its-amazing-that-federal-programs-work-at-all-this-being-a-saga-of-the-economic-development-administration-as-told-by-two-sympathetic-observers-who-seek-to-build-morals-on-a-foundation-of-ruined-hopes-by-jeffrey-l-pressman-and-aaron-wildavsky-berkeley-university-of-california-press-1973-pp-xviii-182-750/198F70855A5A084BAE53913F6C211444

Price, Monroe E. *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power*. Cambridge, MA: MIT Press, 2002. https://direct.mit.edu/books/monograph/2029/Media-and-SovereigntyThe-Global-Information

Prime Minister's Office, Republic of Poland. *Strategic Communication Review: Media Sovereignty and National Security*. Warsaw: Prime Minister's Chancellery, 2021. https://www.gov.pl/web/diplomacy/strategic-communication-and-countering-foreign-disinformation

Przeworski, Adam, and Henry Teune. *The Logic of Comparative Social Inquiry*. New York: Wiley, 1970. https://www.researchgate.net/publication/235413195_The_Logic_of_Comparative_Social_Inquiry

Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000. Print.

———. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427-460. https://www.jstor.org/stable/2706785

Pynnöniemi, Katri. "Russia's National Security Strategy: Analysis of Conceptual Evolution." Helsinki: Finnish Institute of International Affairs, 2016. https://www.tandfonline.com/doi/abs/10.1080/13518046.2018.1451091

Pynnöniemi, Katri, and András Rácz. "Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine." Helsinki: Finnish Institute of International Affairs, 2016. https://fiia.fi/en/publication/fog-of-falsehood

Pynnöniemi, Katri, and Tomáš Baranec. "Russia's Hybrid Influence Campaign in the 2021 Belarus Migration Crisis." Helsinki: Finnish Institute of International Affairs, 2022. Print.

Radin, Andrew, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long. "The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition." Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3099/RAND_RR3099.pdf

Raso, Jennifer, and Hannah Bloch-Wehba. "Algorithmic Accountability in the Administrative State." *Yale Journal on Regulation* 37, no. 3 (2020): 800-854. Print.

Rawls, John. *A Theory of Justice*. Cambridge, MA: Harvard University Press, 1971. https://www.jstor.org/stable/j.ctvjf9z6v

Reinhardt, K. "NATO Information Operations and Strategic Communications." *Strategic Studies Quarterly* 7, no. 2 (2003): 45-67. https://nllp.jallc.nato.int/iks/sharing%20public/russian-info-operations-revised-version-digital%20(1).pdf

Renz, Bettina. “Russia and ‘Hybrid Warfare’: Going Beyond the Label.” Helsinki: University of Helsinki, 2016. https://helda.helsinki.fi/server/api/core/bitstreams/9514b166-0249-42a4-a408-9195e7d32292/content

Reuter, Ora John, and David Szakonyi. “Elite Cues and Citizen Compliance with Public Health Measures.” *Journal of Politics* 83, no. 4 (2021): 1562-1577. https://journals.sagepub.com/doi/10.1177/00208345211051898

Reuters Institute for the Study of Journalism. *Digital News Report 2022*. Oxford: University of Oxford, 2022. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022

———. *Digital News Report 2023: Poland Country Overview*. Oxford: University of Oxford, 2023. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023

Ribeiro, Manoel Horta, Raphael Ottoni, Robert West, Virgílio A. F. Almeida, and Wagner Meira Jr. “Auditing Radicalization Pathways on YouTube.” In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 131-141. New York: Association for Computing Machinery, 2020. https://dl.acm.org/doi/10.1145/3351095.3372879

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020. https://www.cia.gov/resources/csi/static/active-measures-and-information-wars.pdf

Roberts, Hal, Yochai Benkler, Robert Faris, Alicia Solow-Niederman, and Ethan Zuckerman. “The State of the Platforms.” Cambridge, MA: Berkman Klein Center for Internet & Society, December 2021. Print.

Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. “The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation.” *AI & Society* 36, no. 1 (2021): 59-77. https://link.springer.com/article/10.1007/s00146-020-00992-2

Roberts, Sarah T. *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven, CT: Yale University Press, 2019. https://www.jstor.org/stable/j.ctvhrcz0v

Robinson, Piers. *The CNN Effect: The Myth of News, Foreign Policy and Intervention*. London: Routledge, 2002. https://www.taylorfrancis.com/books/mono/10.4324/9780203995037/cnn-effect-piers-robinson

Roe, Paul. “Securitization and Minority Rights: Conditions of Desecuritization.” *Security Dialogue* 35, no. 3 (2004): 279-294. https://www.jstor.org/stable/26298626

Roozenbeek, Jon, and Sander van der Linden. “Fake News Game Confers Psychological Resistance Against Online Misinformation.” *Palgrave Communications* 5, no. 65 (2019): 1-10. https://www.nature.com/articles/s41599-019-0279-9

———. “The Fake News Game: Actively Inoculating Against the Risk of Misinformation.” *Journal of Risk Research* 22, no. 5 (2019): 570-580. https://www.tandfonline.com/doi/full/10.1080/13669877.2018.1443491

Roozenbeek, Jon, Sander van der Linden, and Thomas Nygren. “Prebunking Interventions Based on ‘Inoculation’ Theory Can Reduce Susceptibility to Misinformation Across Cultures.” *Harvard Kennedy School Misinformation Review* 1, no. 2 (2020): 1-23. https://misinforeview.hks.harvard.edu/wp-content/uploads/2020/02/FORMATTED_globalvaccination_Jan30.pdf

Rose, Gideon. “Neoclassical Realism and Theories of Foreign Policy.” *World Politics* 51, no. 1 (1998): 144-172. https://ir101.co.uk/wp-content/uploads/2018/11/Rose-Neoclassical-Realism-and-Theories-of-Foreign-Policy.pdf

Rosen, Armin. “Democracy’s Disinformation Dilemma.” *Commentary Magazine*, March 2021. Print.

———. “How Democracies Can Win the Information War.” *The Atlantic*, March 15, 2019. Print.

Rosen, Guy. “An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19.” Menlo Park, CA: Meta Newsroom, April 16, 2020. https://about.fb.com/news/2020/04/covid-19-misinfo-update/

Rosenau, James N. *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton, NJ: Princeton University Press, 1990. https://www.jstor.org/stable/j.ctv301hg5

Rumsfeld, Donald. “Global War on Terrorism Strategic Communication Assessment.” Washington, D.C.: Department of Defense, October 16, 2006. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2025/Communication-Strategery/

Russell, Stuart J., Daniel Dewey, and Max Tegmark. “Research Priorities for Robust and Beneficial Artificial Intelligence.” *AI Magazine* 36, no. 4 (2015): 105-114. https://futureoflife.org/data/documents/research_priorities.pdf

Said, Edward W. *Orientalism*. New York: Pantheon Books, 1978. https://monoskop.org/images/4/4e/Said_Edward_Orientalism_1979.pdf

Scharre, Paul. “Deepfakes and the Coming AI Dystopia.” *War on the Rocks*, February 15, 2019. Print.

Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960. https://www.sackett.net/Strategy-of-Conflict.pdf

Schmidt, Vivien A. *The Futures of European Capitalism*. Oxford: Oxford University Press, 2002. https://academic.oup.com/book/9931

Scopus. “Global Research Trends in Disinformation Studies 2018-2023.” Amsterdam: Elsevier, 2023. Print.

Searle, John R. *The Construction of Social Reality*. New York: Free Press, 1995. https://epistemh.pbworks.com/f/6.+The+Construction+of+Social+Reality+(SCAN).pdf

Secrétariat Général de la Défense et de la Sécurité Nationale. *Revue Stratégique de Cyberdéfense*. Paris: République Française, 2018. https://www.sgdsn.gouv.fr/publications/revue-strategique-de-cyberdefense

Seib, Philip. *Real-Time Diplomacy: Politics and Power in the Social Media Era*. New York: Palgrave Macmillan, 2012. https://link.springer.com/book/10.1057/9781137010902

Sen, Amartya. *Development as Freedom*. New York: Knopf, 1999. https://kuangaliablog.wordpress.com/wp-content/uploads/2017/07/amartya_kumar_sen_development_as_freedombookfi.pdf

Senate of Poland. “Ustawa o radiofonii i telewizji - Lex TVN.” Warsaw: Senate of Poland, September 11, 2021. https://www.prawo.pl/biznes/przesuniety-termin-wejscia-w-zycie-lextvn,509976.html

Sénat. *Rapport d’Information sur la Lutte contre l’Influence Informatique d’Ingérence*. Commission des Affaires Étrangères, de la Défense et des Forces Armées. Paris: Sénat, 2024. https://www.senat.fr/rap/r23-739-1/r23-739-1.html

———. *Rapport d’Information sur la Souveraineté Numérique*. Commission des Affaires Européennes. Paris: Sénat, 2020. https://www.senat.fr/travaux-parlementaires/structures-temporaires/commissions-denquete/commissions-denquete/commission-denquete-sur-la-souverainete-numerique.html

Service VIGINUM. *Rapport sur les Ingérences Numériques Étrangères lors de l’Élection Présidentielle 2022*. Paris: République Française, 2022. https://www.vie-publique.fr/en-bref/286939-viginum-cas-dingerences-etrangeres-en-ligne-detectes-elections-2022

Shambaugh, David. “China’s Soft-Power Push: The Search for Respect.” *Foreign Affairs* 94, no. 4 (2015): 99-107. https://www.jstor.org/stable/24483821

Shearer, Elisa, and Elizabeth Grieco. “Americans Are Wary of the Role Social Media Sites Play in Delivering the News.” Washington, D.C.: Pew Research Center, October 2019. https://www.pewresearch.org/journalism/2019/10/02/americans-are-wary-of-the-role-social-media-sites-play-in-delivering-the-news/

Shekhovtsov, Anton. “Russian Disinformation and the Weaponization of European Grievances.” In *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, 112-128. London: Routledge, 2020. Print.

Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Press, 2008. https://techofcomm.wordpress.com/wp-content/uploads/2015/11/here_comes_everybody_power_of_organizing_without_organizations.pdf

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014. https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918119

Smith, Tony. *America’s Mission: The United States and the Worldwide Struggle for Democracy*. Princeton, NJ: Princeton University Press, 1994. https://www.jstor.org/stable/j.ctt7s360

Snegovaya, Maria. “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare.” Washington, D.C.: Institute for the Study of War, September 2015. https://www.files.ethz.ch/isn/193932/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Snow, Nancy. *Propaganda, Inc.: Selling America’s Culture to the World*. New York: Seven Stories Press, 2002. https://archive.org/details/propagandaincsel0000snow_b1r9

Snowden, Edward. *Permanent Record*. New York: Metropolitan Books, 2019. https://avalonlibrary.net/ebooks/Edward%20Snowden%20-%20Permanent%20Record.pdf

Snyder, Glenn H. *Alliance Politics*. Ithaca, NY: Cornell University Press, 1997. https://academic.oup.com/psq/article-abstract/113/3/513/6962186?redirectedFrom=PDF

Stamos, Alex. “Information Operations and Facebook.” Stanford, CA: Center for International Security and Cooperation, Stanford University, 2019. https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf

Stanley, Jason. *How Fascism Works: The Politics of Us and Them*. New York: Random House, 2018. https://blackbooksdotpub.wordpress.com/wp-content/uploads/2021/05/jason-stanley-how-fascism-works_-the-politics-of-us-and-them-random-house-2018.pdf

Starbird, Kate. "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (2019): 1-26. https://dl.acm.org/doi/10.1145/3359229

———. "Disinformation's Spread: Bots, Trolls and All of Us." *Nature* 571, no. 7766 (2019): 449. https://www.nature.com/articles/d41586-019-02235-x

Starbird, Kate, Ahmer Arif, and Tom Wilson. "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (2019): 1-26. https://dl.acm.org/doi/10.1145/3359229

State Department. "Strategic Communication and Public Diplomacy Policy Coordinating Committee." Washington, D.C.: Department of State, 2006. https://www.gao.gov/products/gao-07-904

Stefan Batory Foundation. *Civil Society Under Pressure: Annual Report 2023*. Warsaw: Batory Foundation, 2023. Print.

Stiegler, Bernard. *De la Disruption: Comment ne pas Devenir Fou?* Paris: Les Liens qui Libèrent, 2019. https://hal.science/hal-03789329v1/document#:~:text=Philosopher%20pour%20ne%20pas%20devenir%20fou%20%C2%BB%2C%20l'auteur%20d%C3%A9finit,24).

Stigler, George J. "The Theory of Economic Regulation." *The Bell Journal of Economics and Management Science* 2, no. 1 (1971): 3-21. https://www.jstor.org/stable/3003160

Stone, Geoffrey R. *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*. New York: W.W. Norton, 2004. https://chicagounbound.uchicago.edu/books/178/

Streeck, Wolfgang, and Kathleen Thelen, eds. *Beyond Continuity: Institutional Change in Advanced Political Economies*. Oxford: Oxford University Press, 2005. https://academic.oup.com/book/54803

Suleiman, Ezra N. *Elites in French Society: The Politics of Survival*. Princeton, NJ: Princeton University Press, 1978. https://www.jstor.org/stable/j.ctt13x1dw8

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. “Technology, Autonomy, and Manipulation.” *Internet Policy Review* 8, no. 2 (2019): 1-22. https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation

Taguba, Antonio M. “Article 15-6 Investigation of the 800th Military Police Brigade.” Washington, D.C.: U.S. Army, 2004. https://hrlibrary.umn.edu/OathBetrayed/Taguba-Report.pdf

Taguieff, Pierre-André. *La République Enlisée: Pluralisme, Communautarisme et Citoyenneté*. Paris: Éditions des Syrtes, 2001. Print.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007. https://budisetiawanjr.wordpress.com/wp-content/uploads/2020/03/the-black-swan_-the-impact-of-the-highly-improbable-second-edition-pdfdrive.com-.pdf

Taussig, Sylvie. “L’État et la Laïcité: Enjeux Contemporains.” *Revue de Droit Public* 135, no. 3 (2019): 675-692. Print.

Thelen, Kathleen. *How Institutions Evolve: The Political Economy of Skills in Germany, Britain, the United States, and Japan*. Cambridge: Cambridge University Press, 2004. https://www.cambridge.org/core/books/how-institutions-evolve/41C3108269725FA3AF2C4AE87A50685E

Thomas, Timothy L. “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256. http://impiousdigest.com/wp-content/uploads/2017/08/Thomas_2004.pdf

Thornton, Rod. “The Changing Nature of Modern Warfare: Responding to Russian Information Warfare.” *The RUSI Journal* 160, no. 4 (2015): 40-48. https://www.rusi.org/explore-our-research/publications/rusi-journal/changing-nature-modern-warfare-responding-russian-information-warfare

Tizard, John. “Cybernetic Strategic Communication: Real-Time Feedback Systems in Digital Influence Operations.” *Strategic Studies Quarterly* 17, no. 2 (2023): 89-112. Print.

Tsebelis, George. *Veto Players: How Political Institutions Work*. Princeton, NJ: Princeton University Press, 2002. https://www.jstor.org/stable/j.ctt7rvv7

Tsygankov, A. P. *Russia’s Foreign Policy: Change and Continuity in National Identity*. Lanham, MD: Rowman & Littlefield, 2006. https://archive.org/details/russiasforeignpo0000tsyg_c5y0

Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." Menlo Park, CA: Hewlett Foundation, March 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139

Tufekci, Zeynep. "Algorithmic Amplification of Politics on Twitter." *Proceedings of the National Academy of Sciences* 119, no. 1 (2022): e2025334119. Print.

———. "Engineering the Public: Big Data, Surveillance and Computational Politics." *First Monday* 19, no. 7 (2014): 1-12. https://medialaw.unc.edu/wp-content/uploads/2013/10/DRAFT-Engineering-the-Public-by-Zeynep-Tufekci.pdf

———. "YouTube, the Great Radicalizer." *New York Times*, March 10, 2018. https://www.niemanlab.org/reading/youtube-the-great-radicalizer/

Twitter, Inc. *Transparency Report: Content Moderation*. San Francisco: Twitter, Inc., 2022. https://transparency.x.com/content/dam/transparency-twitter/2025/x-global-transparency-report_h2_2024.pdf

Ullman, Harlan K., and James P. Wade. *Shock and Awe: Achieving Rapid Dominance*. Washington, D.C.: National Defense University Press, 1996. http://www.dodccrp.org/files/Ullman_Shock.pdf

United Nations Office for Disarmament Affairs. "Developments in the Field of Information and Telecommunications in the Context of International Security." New York: United Nations, 2024. https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context

University of Warsaw. "Border Communities and Information Resilience Survey." Warsaw: Institute of Sociology, University of Warsaw, 2022. Print.

U.S. Army. *Field Manual 3-24: Counterinsurgency*. Washington, D.C.: Headquarters, Department of the Army, 2018. https://irp.fas.org/doddir/army/fm3-24.pdf

U.S. Congress. "Clarifying Lawful Overseas Use of Data Act (CLOUD Act)." H.R. 4943, 115th Congress, 2018. https://www.eurojust.europa.eu/publication/cloud-act

U.S. Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command." Fort Meade, MD: U.S. Cyber Command, April 2018. https://mail.stratml.us/pdfs/USCYBERCOM.pdf

U.S. Department of Defense. “Joint Doctrine Note 1-20: Information in the Joint Environment.” Washington, D.C.: Department of Defense, April 24, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

U.S. Department of Homeland Security. “DHS Pauses Work of Disinformation Governance Board.” Washington, D.C.: DHS, May 18, 2022. https://www.cbsnews.com/video/dhs-pauses-work-of-disinformation-governance-board/

———. “Summary of Terrorism Threat to the U.S. Homeland.” National Terrorism Advisory System Bulletin. Washington, D.C.: DHS, February 7, 2022. https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-august-13-2021

U.S. Department of Justice. “January 6th Capitol Breach Cases.” Washington, D.C.: DOJ Criminal Division, 2023. https://www.justice.gov/archives/opa/speech/deputy-assistant-attorney-general-lisa-h-miller-delivers-remarks-university-southern

U.S. Department of State. “Global Engagement Center.” Fact Sheet, Bureau of Global Public Affairs. Washington, D.C.: Department of State, March 2018. https://2021-2025.state.gov/about-us-global-engagement-center-2/

———. *Pillars of Russia’s Disinformation and Propaganda Ecosystem*. Washington, D.C.: Global Engagement Center, 2020. https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

———. “Statement on Poland’s Holocaust Law.” Press Statement. Washington, D.C.: Department of State, February 2018. Print.

———. “Strategic Plan FY 2022-2026.” Bureau of Global Public Affairs. Washington, D.C.: Department of State, 2022. https://www.state.gov/wp-content/uploads/2022/03/Final-State-USAID-FY-2022-2026-Joint-Strategic-Plan_29MAR2022.pdf

U.S. Government Accountability Office. “Artificial Intelligence: Federal Coordination Challenges and Opportunities.” GAO Report 24-105. Washington, D.C.: GAO, March 2024. https://www.gao.gov/products/gao-18-644t

———. “Strategic Communication: Federal Coordination Challenges and Opportunities.” GAO Report 21-234. Washington, D.C.: GAO, March 2021. Print.

U.S. House Select Committee to Investigate the January 6th Attack on the United States Capitol. *Final Report*. 117th Congress. Washington, D.C.: U.S. House of Representatives, 2022. https://www.govinfo.gov/content/pkg/GPO-J6-REPORT/pdf/GPO-J6-REPORT.pdf

U.S. Joint Chiefs of Staff. "Joint Publication 3-13: Information Operations." Washington, D.C.: Department of Defense, November 20, 2014. https://www.researchgate.net/publication/305680531_Joint_Publication_3-13_Information_Operations

———. "Joint Publication 3-13: Information Operations." Washington, D.C.: Department of Defense, 2006. Print.

U.S. Senate Committee on Homeland Security and Governmental Affairs and Committee on Rules and Administration. *Examining the January 6 Attack on the U.S. Capitol*. 117th Congress. Washington, D.C.: U.S. Senate, 2021. https://www.rules.senate.gov/imo/media/doc/Jan%206%20HSGAC%20Rules%20Report.pdf

U.S. Senate Select Committee on Intelligence. *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. 5 vols. 116th Congress. Washington, D.C.: U.S. Senate, 2020. https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-united-states-senate-russian-active-measures/

Vachudova, Milada Anna. *Europe Undivided: Democracy, Leverage, and Integration After Communism*. Oxford: Oxford University Press, 2005. https://archive.org/details/europeundividedd0000vach

Vaccari, Cristian, and Andrew Chadwick. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society* 6, no. 1 (2020): 1-13. https://journals.sagepub.com/doi/10.1177/2056305120903408

Vaïsse, Maurice. *La Grandeur: Politique étrangère du général de Gaulle, 1958-1969*. Paris: Fayard, 1998. https://www.fayard.fr/livre/la-grandeur-9782213600505/

Vakil, Sanam. "Iran's Use of Shi'i Militia Proxies." London: Chatham House, December 2018. https://www.mei.edu/sites/default/files/publications/Vatanka_PolicyPaper.pdf

van der Linden, Sander, Jon Roozenbeek, and Josh Compton. "Inoculating Against Fake News About COVID-19." *Frontiers in Psychology* 11 (2020): 566790. https://pmc.ncbi.nlm.nih.gov/articles/PMC7644779/

van Dijck, José. *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press, 2013. https://academic.oup.com/book/9914

Vilmer, Jean-Baptiste Jeangène. "The 'Cognitive Warfare' Label: Blurring the Lines Between Academic Research and Defense Concerns." *War on the Rocks*, December 2021. Print.

———. "The 'MacronLeaks' Operation: A Post-Mortem." Washington, D.C.: Atlantic Council, June 2019. https://rsis.edu.sg/wp-content/uploads/2020/03/PR200325_Securing-Elections-and-Beyond.pdf

Virilio, Paul. *Speed and Politics: An Essay on Dromology*. New York: Semiotext(e), 1986. https://monoskop.org/images/archive/c/c1/20170626060354%21Virilio_Paul_Speed_and_Politics_2006.pdf

Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (2018): 1146-1151. https://ide.mit.edu/wp-content/uploads/2018/12/2017-IDE-Research-Brief-False-News.pdf

Waddington, David. *Policing Public Disorder: Theory and Practice*. Cullompton, UK: Willan Publishing, 2007. https://academic.oup.com/policing/article-abstract/1/4/526/1440967

Wallander, Celeste A. "Institutional Assets and Adaptability: NATO After the Cold War." *International Organization* 54, no. 4 (2000): 705-735. https://www.cambridge.org/core/journals/international-organization/article/abs/institutional-assets-and-adaptability-nato-after-the-cold-war/23C0990675AD899825BE01EDE04CF131

Walt, Stephen M. "The Renaissance of Security Studies." *International Studies Quarterly* 35, no. 2 (1991): 211-239. https://www.jstor.org/stable/2600471

Waltz, Kenneth N. "The Anarchic Structure of World Politics." In *Theory of International Politics*, 88-128. Reading, MA: Addison-Wesley, 1979. https://www.scribd.com/document/370047730/The-Anarchic-Structure-of-World-Politics

———. *Theory of International Politics*. Boston: McGraw-Hill, 1979. https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf

Wang, Sheng-Yu, Oliver Wang, Richard Zhang, Andrew Owens, and Alexei A. Efros. "CNN-Generated Images Are Surprisingly Easy to Spot... for Now." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 1-10. Los Alamitos, CA: IEEE, 2020. https://arxiv.org/abs/1912.11035

Wardle, Claire, and Hossein Derakhshan. “Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.” Council of Europe Report DGI(2017)09. Strasbourg: Council of Europe, September 2017. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

Wendt, Alexander. “Anarchy is What States Make of It: The Social Construction of Power Politics.” *International Organization* 46, no. 2 (1992): 391-425. https://www.jstor.org/stable/2706858

———. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999. http://www.guillaumenicaise.com/wp-content/uploads/2013/10/Wendt-Social-Theory-of-International-Politics.pdf

Wheeler, N. J. *Saving Strangers: Humanitarian Intervention in International Society*. Oxford: Oxford University Press, 2000. https://academic.oup.com/book/276/chapter-abstract/134833794?redirectedFrom=fulltext

White House. *The National Security Strategy of the United States of America*. Washington, D.C.: White House, 2002. https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/

Wigell, Mikael. “Democratic Deterrence: How to Dissuade Hybrid Interference.” *Washington Quarterly* 44, no. 1 (2021): 49-67. https://www.tandfonline.com/doi/full/10.1080/0163660X.2021.1893027

Wigell, Mikael, Sören Scholvin, and Minna Aaltola, eds. *Geo-economics and Power Politics in the 21st Century: The Revival of Economic Statecraft*. London: Routledge, 2018. Print.

Wildavsky, Aaron. *Searching for Safety*. New Brunswick, NJ: Transaction Publishers, 1988. https://www.academia.edu/1811938/Searching_for_safety

Wilson, Jameson, and Sarah Starbird. “Cross-Platform Information Operations and the ‘Plandemic’ Conspiracy Theory.” *Harvard Kennedy School Misinformation Review* 2, no. 1 (2021): 1-18. https://misinforeview.hks.harvard.edu/wp-content/uploads/2020/01/V2_starbird_crossplatform_jan29.pdf

Wilson, Steven Lloyd, and Charles Wiysonge. “Social Media and Vaccine Hesitancy.” *BMJ Global Health* 5, no. 10 (2020). https://pubmed.ncbi.nlm.nih.gov/33097547/

Winner, Langdon. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MA: MIT Press, 1977. https://archive.org/details/ETC0963

Winner, Langdon. “Do Artifacts Have Politics?” *Daedalus* 109, no. 1 (1980): 121-136. https://faculty.cc.gatech.edu/~beki/cs4001/Winner.pdf

Wohlforth, William C. “The Stability of a Unipolar World.” *International Security* 24, no. 1 (1999): 5-41. https://www.belfercenter.org/publication/stability-unipolar-world

World Health Organization. “Novel Coronavirus (2019-nCoV): Situation Report - 13.” Geneva: WHO, February 2, 2020. https://reliefweb.int/report/china/novel-coronavirus-2019-ncov-situation-report-13-2-february-2020

World Health Organization Emergency Committee. “Statement on the Second Meeting of the International Health Regulations Emergency Committee Regarding the Outbreak of Novel Coronavirus (2019-nCoV).” Geneva: WHO, January 30, 2020. https://georgia.un.org/en/47774-statement-second-meeting-international-health-regulations-emergency-committee-regarding

World Intellectual Property Organization. “WIPO Technology Trends 2023: Artificial Intelligence.” Geneva: WIPO, 2023. Print.

Wæver, Ole. “Securitization and Desecuritization.” In *On Security*, edited by Ronnie D. Lipschutz, 46-86. New York: Columbia University Press, 1995. https://dl1.cuni.cz/pluginfile.php/872615/mod_resource/content/1/Waever.pdf

Young, Oran R. *The Effectiveness of International Environmental Regimes: Causal Connections and Behavioral Mechanisms*. Cambridge, MA: MIT Press, 1999. https://mitpress.mit.edu/9780262740234/the-effectiveness-of-international-environmental-regimes/

Zakaria, Fareed. “The Rise of Illiberal Democracy.” *Foreign Affairs* 76, no. 6 (1997): 22-43. https://msuweb.montclair.edu/~lebelp/fzakariailliberaldemocracy1997.pdf

Zarocostas, John. “How to Fight an Infodemic.” *The Lancet* 395, no. 10225 (2020): 676. https://pubmed.ncbi.nlm.nih.gov/32113495/

Zarycki, Tomasz. *Ideologies of Eastness in Central and Eastern Europe*. London: Routledge, 2014. https://www.researchgate.net/publication/259603140_Ideologies_of_Eastness_in_Central_and_Eastern_Europe

Zayani, Mohamed, ed. *The Al Jazeera Phenomenon: Critical Perspectives on New Arab Media*. Boulder, CO: Paradigm Publishers, 2005. https://www.plutobooks.com/product/the-al-jazeera-phenomenon/

Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press, 1999. https://www.cia.gov/resources/csi/static/flawed-by-design-creating-secret-state.pdf

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014. https://archive.org/details/countdowntozerod0000zett

Zhang, Feng. "Chinese Hegemony and the Economics of Soft Power." *Review of International Studies* 34, no. 4 (2008): 809-830. https://sk.sagepub.com/book/mono/analysing-chinas-soft-power-strategy-and-comparative-indian-initiatives/chpt/2-chinese-soft-power-historical-background-contemporary#_=_

Zhang, Xiaoling. "Chinese Discourse Power: Aspirations and Reality." *Asian Survey* 58, no. 6 (2018): 1039-1062. Print.

Zielonka, Jan. "How New Enlarged Borders Will Reshape the European Union." *Journal of Common Market Studies* 39, no. 3 (2001): 507-536. https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5965.00301

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791

———. "The Coup We Are Not Talking About." *New York Times*, January 29, 2021. https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html

Zuckerberg, Mark. "Congressional Testimony Before the House Committee on Energy and Commerce." Washington, D.C.: U.S. House of Representatives, March 25, 2021. https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/

———. "Testimony Before the House Committee on Energy and Commerce." Washington, D.C.: U.S. House of Representatives, October 2023. Print.

Zwitter, Andrej. "The Ethics of Information Technologies: A Systematic Review of the Moral Implications of ICT." *AI & Society* 36, no. 1 (2021): 271-285. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553758