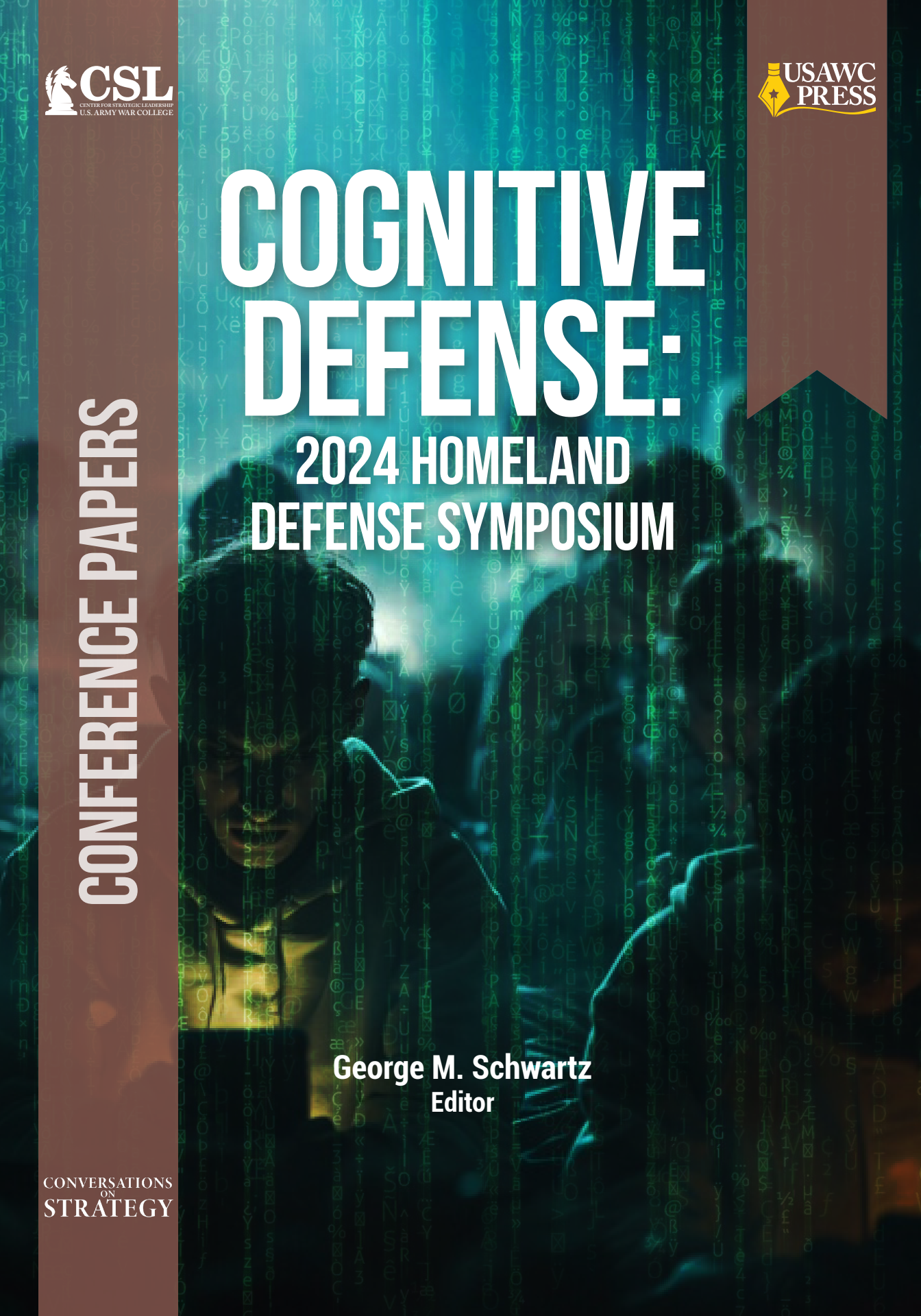
CSL
CENTER FOR STRATEGIC LEADERSHIP
U.S. ARMY WAR COLLEGE

USAWC PRESS

COGNITIVE DEFENSE:

2024 HOMELAND DEFENSE SYMPOSIUM

CONFERENCE PAPERS



George M. Schwartz
Editor

CONVERSATIONS ON STRATEGY

"The Army's Think Tank"

The Strategic Studies Institute (SSI) is the US Army's institute for geostrategic and national security research and analysis. SSI research and analysis creates and advances knowledge to influence solutions for national security problems facing the Army and the nation.

SSI serves as a valuable source of ideas, criticism, innovative approaches, and independent analyses as well as a venue to expose external audiences to the US Army's contributions to the nation. It acts as a bridge to the broader international community of security scholars and practitioners.

SSI is composed of civilian research professors, uniformed military officers, and a professional support staff, all with extensive credentials and experience. SSI's Strategic Research and Analysis Department focuses on global, transregional, and functional security issues. Its Strategic Engagement Program creates and sustains partnerships with strategic analysts around the world, including the foremost thinkers in the field of security and military strategy. In most years, about half of SSI's publications are written by these external partners.

Research Focus Arenas

Geostrategic net assessment—regional and transregional threat analysis; drivers of adversary conduct; interoperability between partners, allied, IA, commercial, and Joint organizations

Geostrategic forecasting—geopolitics, geoeconomics, technological development, and disruption and innovation

Applied strategic art—warfare and war-fighting functions, Joint and multinational campaigning, and spectrum of conflict

Industrial/enterprise management, leadership, and innovation—ethics and the profession, organizational culture and effectiveness, transformational change, talent development and management, and force mobilization and modernization

Cognitive Defense:
2024 Homeland Defense Symposium

George M. Schwartz, Editor

June 2025

USAWC PRESS
US ARMY WAR COLLEGE

Strategic Studies Institute

Comments pertaining to this publication are invited and should be forwarded to: Director, Strategic Studies Institute and US Army War College Press, US Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

******

ISBN 1-58487-864-9

Cover Image Credits

Image description: View of people addicted to their smarphonte

Image created by: Freepik

Website: https://www.freepik.com/free-ai-image/view-people-addicted-their-smartphone-looking-scrolling-through-screens_186027245.htm

Image description: Freepick image extended with Photoshop generative AI and overlaid with an image of "Matrix" from Pixabay

Website: https://pixabay.com/illustrations/matrix-code-computer-pc-data-356024/

Foreword

The term "cognitive defense" is gaining traction in national security and homeland-defense planning. And for good reason. The diverse portfolio of threats to the homeland that has emerged following two decades of conflict in the Middle East and Southwest Asia, a resurgent and aggressive Russia, and the pacing competition from China overlays a range of domestic challenges and advanced technologies with the potential to serve as threat enablers. Defending the homeland to secure US interests domestically and abroad has taken on relatively sudden and significant importance, as the away game now clearly begins inside the borders of the United States and our allies and involves a comprehensive civil-society component as well.

The Homeland Defense Symposium was truly fortunate to have distinguished members of the defense, homeland security, and academic communities share their views and experience. As you will see in the following pages, the participants' combined thoughts provide a thoughtful review of cognitive defense and how we—collectively—might apply an understanding of cognitive defense to meet the array of challenges and opportunities ahead. Major-General Darcy Molstad, deputy commander of the Canadian Joint Operations Command, set the scene with a global context, discussing the origins of cognitive warfare and how relevant doctrine has evolved and been applied in NATO planning, which defines the term as follows.

> Activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage . . . . Cognitive Warfare integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other Instruments of Power, can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary.

The definitions of the operational side of cognitive defense provided the backdrop for complementary presentations by Dr. George Schwartz, director of the Emergency Planning and Management program at Immaculata University and former assistant adjutant general of the Pennsylvania National Guard (and current faculty member at the US Army War College); Dr. Michael Roi, strategic adviser to the Canadian Joint Operations Command and former head

of the defense planning team in the office of the Canadian assistant deputy minister (policy); and Dr. Mark Landahl, emergency manager for the city of Rockville, Maryland, and former homeland security commander for the Frederick County Sheriff's Office. Together, the speakers described the complexity of defending against nonkinetic threats. The challenges, as you will read, reside mainly in how we might strengthen our collective resilience in the face of competitors and adversaries using cognitive warfare as an enabling element of their defense and security actions.

Our hope is the following papers will engage you in exploring, understanding, and applying their respective critical analyses of cognitive defense. On behalf of the distinguished speakers and the Naval Postgraduate School Center for Homeland Defense and Security, congratulations to the US Army War College, Center for Strategic Leadership for hosting this timely and worthwhile event. The Center for Homeland Defense and Security was honored to contribute alongside our partners at the US Army War College and the Homeland Defense Institute.

Steve Recca
Director
University and Agency Partnership Program
Center for Homeland Defense and Security
Naval Postgraduate School

Executive Summary

The Homeland Defense and Security Issues Group from the Center for Strategic Leadership at the US Army War College hosted the inaugural Homeland Defense Symposium at Carlisle Barracks, Pennsylvania from February 6 to 8, 2024. The theme of this first annual conference was "Reestablishing the Sanctuary," which reflects the recognition among the participants that the homeland is already threatened and will be a theater of action in any future large-scale combat operation.

Indeed, the final panel, organized by the Center for Homeland Defense and Security at the Naval Postgraduate School, highlighted how potential adversaries are already conducting operations in the United States and Canada to prepare for a future conflict. Using disinformation and social media means, cognitive warfare seeks to shape the attitudes and behaviors of a civilian populace by negatively influencing and disrupting their cognitive processes to weaken a society's political will and degrade national resilience. In the current phase of global competition, our potential adversaries are attacking the minds of Americans as well as those of our Canadian and European allies.

The panelists who authored these papers have a broad range of experience in homeland security and with the US and Canadian militaries. The panelists provide insights and offer solutions for cognitive defense. As elaborated in the conference papers, some key takeaways include the following.

- Cognitive warfare is not new and can be explained using Carl von Clausewitz's paradoxical trinity, for example. But open access to information from anywhere in the world through mobile technology and social media has created a more pernicious threat that is causing a loss of trust in institutions, which can undermine national will during a crisis.

- Disinformation operations by foreign and domestic extremist actors are leveraging events that can generate a lot of emotion, such as elections and disasters, to confuse public perceptions and create societal schisms.

- The legal frameworks for responding to disinformation campaigns in the homeland are uncertain, and legislative action is needed to provide civil authorities with effective countermeasures.

- The North Atlantic Treaty Organization (NATO) has been examining the concept of cognitive warfare and offers some approaches that can be adopted in North America. One of NATO's newest member countries, Finland, has been using a whole-of-society strategy to deal with Russian disinformation for years.

- The US and Canadian governments need to take a more active role in defending the cognitive domain by developing comprehensive strategies. The US National Preparedness System, for example, provides a structure that can be adapted to address the threat of cognitive warfare.

— 1 —

Cognitive Defense: A Case Study of Hyperlocal Impacts of Information Operations in Domestic Incident Response

Mark Landahl, PhD

ABSTRACT: Adversary information operations against the United States extend beyond significant political events, such as elections, to impact the domestic response to disasters. Information operations by foreign and domestic-extremist actors during the East Palestine, Ohio, train derailment show the scope of the problem and the potential for disruption. This chapter reviews the response to information operations in the domestic context, examining the legal framework and current legislative considerations. The chapter discusses issues related to managing misinformation, disinformation, and malinformation in the context of domestic response operations, with a focus on effective countermeasures.

Introduction

Information operations by foreign actors came to public light as a strategic surprise during the 2016 US presidential election cycle.[1] Foreign information operations continued in efforts to influence the 2018 and 2020 elections.[2] The reach and scope of information operations by foreign and domestic actors have pushed into the realm of domestic disaster response. Though disconnected from international events, domestic disasters present the opportunity for adversaries to foment distrust and erode unity across levels of the US government, including impacts down to the lowest level of local government. Although observed in many events, including the recent Maui wildfires of 2023, this chapter will examine information operations and their impacts through the lens of the response to the East Palestine, Ohio,

train derailment on February 3, 2023.[3] This chapter will (1) define and categorize information operations in the context of the homeland; (2) contextualize the threat through the examination of homeland-related threat statements; (3) provide an overview of the East Palestine, Ohio, train derailment; (4) detail information operations undertaken during the incident; and (5) examine countermeasures to information operations for domestic incident response.

Defining Information Operations in the Homeland

The US Department of Defense identifies information operations as those which intend to "influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[4] In the context of the homeland, the US Department of Homeland Security (DHS) *Homeland Threat Assessment 2024* (HTA) categorizes foreign information operations into three types based on intention.[5] Table 1-1 details the categories and provides descriptions of misinformation, disinformation, and malinformation.[6]

Table 1-1. DHS HTA types of information operations

Type	Description
Misinformation	false, inaccurate, or misleading information that is spread regardless of the intent to deceive
Disinformation	false or misleading information that is deliberately created or spread with the intent to deceive or mislead
Malinformation	deliberate use of otherwise verifiable information with malicious intent, such as by amplifying the information selectively, out of context, or to the detriment of specific persons

The definitions in table 1-1 provide a frame for the type of information activities adversaries may employ in the homeland. This context frames the examination of information operations in the response to the East Palestine, Ohio, train derailment.

Contextualizing the Threat Landscape

The Office of the Director of National Intelligence's 2024 *Annual Threat Assessment of the U.S. Intelligence Community* and the DHS HTA present the current unclassified threat picture for the United States.[7] The previous section presented the HTA lexicon to frame information operations in the homeland. Before examining

the threat content in the assessments, some distinction must be drawn between how information operations are described across the two assessments. In contrast to the HTA, the Office of the Director of National Intelligence uses the term influence operations in the assessment to describe information-operations activities, using the terms misinformation, disinformation, and malign influence.[8] Malign influence is codified in law in 50 US Code § 3059(e)(2) and defined as:

> any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means—(A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States.[9]

The Office of the Director of National Intelligence's assessment identifies malign-influence activities in the contested cyberspace by the states of Russia, China, and Iran and topically in the context of post–COVID-19 health security. The assessment identifies specific health-related misinformation efforts that seek to create doubt and undermine global institutions focused on public health. Specific to states, the Office of the Director of National Intelligence concludes these activities are "growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval."[10] The Office of the Director of National Intelligence's threat assessment does not address domestic-actor considerations and identifies only nation-states as potential perpetrators of influence operations.

Beyond the typology and definitions, the DHS HTA identifies, "Nation-state adversaries intent on undermining our social cohesion are incorporating new technologies into their mis-, dis-, and malinformation campaigns, which will likely ramp up ahead of the elections this year."[11] The DHS HTA also explicitly identifies potential activities by China and Russia related to information operations. Chinese government influence activities "likely will continue their efforts to refine and employ tactics and messaging to influence US discourse."[12] The DHS HTA describes Russia "likely will continue to use traditional media, covert websites, social networks, online bots, trolls, and individuals to amplify pro-Kremlin narratives and conduct influence activities within the United States. Since its invasion of Ukraine, Russian messaging has focused on justifying its aggression, seeking to reduce US domestic support for Kyiv, and encouraging divisions among the diverse set of global partners that are helping Ukraine."[13]

The HTA also does not identify information operations by domestic actors. Perhaps this issue is almost impossible to untangle from constitutionally protected speech. Later, this chapter discusses the issue further.

Background: East Palestine, Ohio, Train Derailment

On February 3, 2023, a Norfolk Southern Corporation train carrying 20 cars of combustible hazardous materials derailed in East Palestine, Ohio. East Palestine is a rural community of 5,000 residents in Columbiana County in eastern Ohio. The derailment location was just one-fourth of a mile from the Pennsylvania state line and 20 miles from the Ohio River.

Thirty-eight cars were derailed, including 11 tank cars loaded with hazardous materials that resulted in combustion. The fire damaged 12 additional railcars that remained on the tracks. The derailment resulted in a fire and in the release of the hazardous chemical vinyl chloride monomer. The initial response resulted in a one-mile evacuation zone affecting 2,000 residents.[14]

On February 5, 2023, the fires had been extinguished, but concern about a potential explosion grew because of rising temperatures within one of the vinyl-chloride cars.[15] The governor of Ohio activated the National Guard to assist local authorities. Hazardous-materials responders scheduled a controlled venting and burn of five vinyl-chloride cars to mitigate the explosion hazard. Because of the risk, the evacuation area was increased to a one-mile by two-mile area, and the controlled burn was initiated on the afternoon of February 6, 2023.[16]

On February 8, 2023, authorities advised residents they could return to their homes.[17] Although environmental concerns persisted, a containment area was created to remediate soil and water contamination. By February 10, 2023, the US Environmental Protection Agency notified Norfolk Southern Corporation butyl acrylate, ethylhexyl acrylate, and ethylene glycol monobutyl ether were detected in samples from several creeks near the derailment site.[18]

The response at the scene included fire, hazardous-materials, law enforcement, transportation, environmental, and public health personnel from the local (Village of East Palestine) and county (Columbiana) levels, the state of Ohio, the state of Pennsylvania, and the federal government. The response of the state of Ohio included the Ohio Environmental Protection Agency and the Ohio Department of Natural Resources, the Ohio Department of Health, the Ohio State Highway Patrol, the Ohio National Guard, and the Ohio Emergency Management Agency. The state of Pennsylvania's response included the Pennsylvania Department of Environmental Protection and

the Pennsylvania Department of Health. The federal response agencies included the National Transportation Safety Board, the US Department of Transportation, the Environmental Protection Agency, the US Department of Health and Human Services, and the Federal Emergency Management Agency.[19]

President Joe Biden visited the site on February 16, 2024.[20] The state of Ohio continued to release public information bulletins daily through mid-March, with releases of information coming once or twice a week through May 16, 2023.[21] These releases detailed the progress of the cleanup work and the environmental-testing results. The Ohio Environmental Protection Agency shared surface water–sampling results through May 16, 2023, on a dedicated web page. The Environmental Protection Agency continues to share operational updates through the writing of this chapter in September 2024. The National Transportation Safety Board investigation into the incident is also ongoing. The National Transportation Safety Board held hearings in its investigation in East Palestine, Ohio, on June 22–23, 2023.[22] The presentation of the final report and the board vote on the findings on June 25, 2024, indicated an overheated wheel bearing caused the derailment and the vent and burn of the railcars was unnecessary.[23]

Post-Derailment Foreign and Domestic Information Operations

A train derailment in rural eastern Ohio hardly provides the expected backdrop or the Hollywood plotline for foreign information operations. The reality is foreign malign influence became a storyline for the event. This chapter's examination of examples of foreign influence is solely based on open-source reporting and analysis. The incident also was targeted by domestic extremists for information operations. The issue of domestic-extremist information is complex due to the nature of protected speech under the US Constitution. Only narratives with clear extremist ideology are reviewed in the context of mainstream divisive partisan politics.

Foreign Malign Influence Operations

In the early part of the response, foreign malign operations emanating from Russian-linked accounts were identified. The narratives targeted the government response and capitalized on concerns about the speed and capability of the government's response to the incident. Narratives blamed the lack of resources

in the response on the material and resources dedicated to supporting military operations in Ukraine.[24] In addition, narratives pushed conspiracy theories related to the government's suppression of the media. Misinformation is also associated with the scope of the event, the extent of pollution in the Ohio River, and comparisons of the event to the Chernobyl disaster.[25] The narratives also centered on potential conspiracies, including a purportedly suspicious plane crash involving environmental scientists who were responding to the incident—additional messages advanced rumors of a federal shutdown of the area and an occupation of the town.[26]

These narratives are consistent with expectations for foreign malign operations outlined by the Office of the Director of National Intelligence's threat assessment. Although the targeting of limited-scale domestic response operations was not expected, the content and objectives of the operations were targeted. The operations evidence Russian efforts to influence American popular opinion about the Russia-Ukraine War. In addition, the messages also clearly sought to undermine trust in federal and state governments. The nation-state information operations by Russia in East Palestine and, later, Chinese operations during the response to the Maui wildfires of 2023 create concern about future interference with domestic response operations. As a result of these recent interferences, the director of the Federal Emergency Management Agency advised she is very concerned about US adversaries' ability to initiate and spread disinformation, fomenting distrust in government authorities in the wake of domestic incidents such as natural disasters.[27]

Domestic Misinformation, Disinformation, and Malinformation Operations

Partisan political narratives related to the speed and effectiveness of response operations, led by a Republican governor at the state level, and led by a Democratic president at the federal level, permeated First Amendment political discussions around the incident. Partisan political narratives are part of the American political process and are constitutionally protected speech. But within the information exchange around the incident, clear domestic-extremist narratives also emerged.

The Anti-Defamation League identified a series of malinformation narratives that developed, pushing conspiratorial viewpoints, racism, and anti-Semitic themes. Communication associated with the domestic group, the National Justice Party, identified a conspiracy between the government and large corporate rail operators, framing the incident as an attack against White America.[28] The narratives claimed more resources went to supporting incidents such as the Flint water crisis because of the affected minority populations and framed the East Palestine incident

as a fight for White civil rights.[29] Additional narratives claimed, if the area where Governor Mike DeWine lived was the site of the incident, the response would be more urgent and better managed because of a concentrated Jewish population.[30]

The contents of these communications were clearly beyond those of routine partisan divides on domestic issues. The communications advanced conspiracy narratives and incited racial and religious hate. The question in both the foreign and domestic spheres is whether Internet communication channels can or should be regulated by new legislation. The options regarding regulation are examined in the following section of this chapter.

Information-Operations Countermeasures for Domestic Incident Response

Law and Jurisprudence

Countermeasures for foreign malign and domestic-extremist information operations are challenging within the context of American guarantees of free expression. Congress has recently considered legislation to regulate social media companies. The concern is the regulation is equivalent to the controls totalitarian regimes place on Internet content, which the United States routinely criticizes. The US jurisprudence in *New York Times Co. v. Sullivan* (1964) outlined the government may not "regulate false ideas, and even false factual statements receive some constitutional protection."[31] The Supreme Court has accepted the marketplace-of-ideas theory, where all ideas are protected, including false ideas.[32] Common-law applications of defamation and fraud remain, where false and malicious statements of fact can result in civil liability for the harm they cause.[33]

Under current laws, social media companies are not treated equally to traditional media companies. For example, a traditional media company, such as the *Los Angeles Times*, is responsible for the information that appears between its pages (print or electronic), as the company makes editorial choices on the content. The media entity that makes these decisions and publishes content is legally responsible for the content. Under Section 230 of the Communications Decency Act, social media companies are not legally responsible for the content on their platforms because the companies do not decide the content. Most social media companies have developed their own rules for content and try to remove elements that violate established standards.[34] Recent Supreme Court cases challenge this approach and attempt to hold social media companies responsible for content.[35] In the cases

Twitter, Inc. v. Taamneh (2023) and *Gonzalez v. Google* (2023), the families of victims sought to hold the companies responsible for hosting and making available through algorithms, terrorist group–created content that perpetrated attacks resulting in deaths in Paris, France, and Istanbul, Türkiye. The court ruled on the cases on the same day and referenced each case in finding the companies did not "aid and abet" terrorist organizations, preventing claims from being pursued under the Anti-Terrorism Act.[36] The court also ruled claims were barred by Section 230 immunity.[37]

The US Supreme Court also heard oral arguments on March 18, 2024, in *Murthy, Surgeon General, et al. v. Missouri et al.*[38] This case centers on purported federal censorship of social media relating to attempts to control COVID-19 disinformation on social media. The core question before the court is "whether the government's challenged conduct transformed private social-media companies' content-moderation decisions into state action and violated respondents' First Amendment rights."[39] This case did not rest on the interpretation of Section 230 immunity and potential actions taken on behalf of the government, as the ruling was the plaintiffs lacked standing for the case. The ruling stated the plaintiffs failed to show (1) a causal link between the social media restrictions and the actions of government officials and (2) a future injury as a result of the actions of the defendants. The terrorism and COVID-19-related cases in the last year have shaped and reinforced the status of social media under Section 230.

Recent debates and new national legislation have been considered regarding social media companies' use of algorithms. An algorithm is a "specific process or sequence of computational steps followed by a computer in performing a task or problem-solving operation."[40] Legislation has been considered either to bar the use of algorithms or remove Section 230 immunity for companies that use them.[41] The concern is algorithms on social media "may amplify harmful content, create echo-chambers (or filter bubbles) that may contribute to user radicalization and polarization, or drive social media addiction in children."[42] The balance between suppression of speech, reasonable regulation, and liability for companies' harm is a critical current policy debate.[43]

Social Media and Traditional Media in the United States

The right to a free press is guaranteed in the US Constitution's First Amendment. The framers understood a free press was a bulwark against totalitarian control of information, and freedom was impossible without a free press. In the United States, the professional field of journalism has freedom and responsibility

for its content. As described above, the advent of social media has removed responsibility and consequences for some, in an era when everyone considers themselves a journalist.[44]

Journalism as a profession is in trouble. Data from 2021 shows employment in US newsrooms fell by 26 percent from 2008 to 2020, representing a loss of 30,000 jobs.[45] The US Bureau of Labor Statistics predicts the job categories of news analysts, reporters, and journalists will decline by 3 percent from 2022 to 2032.[46] This decline is occurring while the use of social media as a news source grew substantially from 2008 to 2020. Data from 2020 shows 18 percent of Americans used social media for political news.[47] The research also showed those who use social media for news are less engaged, less knowledgeable, and more likely to be exposed to unproven claims.[48]

Most troubling is the growth in using TikTok for news, while most other social media platforms have stagnated or declined.[49] The use of TikTok for news has grown from 3 percent of US adults in 2020 to 14 percent in 2023.[50] On April 24, 2024, President Biden signed the Protecting Americans from Foreign Adversary Controlled Applications Act into law to ban TikTok from the United States, provided the Chinese-owned parent company does not divest its ownership by January 2025. TikTok has filed suit against the government in the District of Columbia Circuit of the US Court of Appeals in the case *TikTok, Inc. v. Garland*. TikTok was banned from federal government devices in 2022 and subsequently banned from government devices in 39 states.[51] A point of concern is 14 percent of US adults are getting their news from a source banned on most government devices across the United States, presenting the challenge of choosing between censorship or maintaining a free market of ideas. The question is whether unregulated and nonliable social media companies and algorithms dictating content exposure are free markets.[52]

Some have advanced the notion broader education for users in information literacy and using critical thinking would improve their identification of sources of misinformation.[53] Others maintain the nature of social media itself makes this approach less likely to be effective. The rewards system for social media ensures posts that are liked or shared result in rewards—be the reward attention or money.[54] Research shows false information spreads faster than accurate information. The more outlandish the information, the more likely the information is to be shared.[55] Other research indicates users sharing misinformation in a viral spread may be more habitual than purposeful.[56] Questions persist about what to do about this problem as legislation related to corporate responsibility for content and potential regulation is under consideration.

Operational-Level Countermeasures

At the point of managing an incident, the debates on political and constitutional grounds and on regulation or liability are moot. Incidents such as the derailment in East Palestine and the Maui wildfires of 2023 will happen while debates on the content of legislation or corporate responsibility for content continue. Until the adoption and implementation of legislation or regulation, those responsible for managing incidents and providing information to the public must work within the current framework. This framework includes possible international and domestic-extremist information operations impacting incident response and recovery. The operational question is: What actions can organizations involved in response and recovery take to communicate with affected populations effectively?

The Department of Homeland Security published a guide entitled *Countering False Information on Social Media in Disasters and Emergencies* in 2018.[57] The guide recommends best practices for people, processes, and technology. For people, the Department of Homeland Security recommends establishing partnerships and relationships with local media and using virtual operations support teams or other technology volunteers to monitor social media activity.[58] The Department of Homeland Security also recommends leveraging trusted influencers and training first responders to identify misinformation.[59] For processes, the guide suggests using the National Incident Management System, Joint Information System protocols for information management; preparing prescripted messages and visuals; engaging actively on social media to address misinformation; engaging in verification processes; and engaging in cross-entity information campaigns.[60] For technology, the guide recommends setting up a central website, using hyperlinks to encourage the sharing of factual information, using live video to correct information, and using monitoring software to identify false information.[61]

Several observable strategies were employed to counter misinformation in the East Palestine incident. Since no after-action report or specific research has been published on actions related to information management and misinformation, the observations in this section are not considered to be a complete understanding of the activities related to the incident. This examination is not intended to be a critique but rather an identification of an area where more specific understanding is needed and an identification of a topic of potential future research.

The first observable strategy was the creation of dedicated websites for incident information by several different agencies with specific technical responsibilities for the incident. At the state level, the Ohio Emergency Management Agency and

the Ohio Environmental Protection Agency created dedicated sites to access the latest information on the incident: the Ohio Emergency Management Agency site archived situation reports and press-conference materials, including video recordings. The Ohio Environmental Protection Agency site publishes environmental-testing data, which continued through the development of this chapter in September 2024. At the federal level, the US Environmental Protection Agency also developed and maintains a dedicated website updated with data through September 2024. The US Centers for Disease Control and Prevention, Agency for Toxic Substances and Disease Registry also has a dedicated site. The National Transportation Safety Board maintains a site on its investigation into the derailment. These sites served as a public repository of accurate information related to specific aspects of the incident. On the private-sector side, the Norfolk Southern Corporation created and maintained a site dedicated to the incident.

The sites dedicated to the incident were limited to other dedicated sites maintained by different agencies. Most connections came from the Ohio Emergency Management Agency site, which is linked to the Ohio Environmental Protection Agency and US Environmental Protection Agency sites for environmental-testing information. The Ohio Emergency Management Agency site did not link to the Centers for Disease Control and Prevention, National Transportation Safety Board, or Norfolk Southern Corporation sites. The Norfolk Southern Corporation site is also linked to the US Environmental Protection Agency and Ohio Environmental Protection Agency testing-result sites. The Ohio Emergency Management Agency site was the most comprehensive, but a single, comprehensive site that linked all components was not created.

The second observable strategy was personal pleas on social media. For example, though Governor DeWine and others had a social media presence, the National Transportation Safety Board Chair Jennifer Homendy took directly to X to post a plea to stop spreading misinformation.[62] Many other strategies were likely employed during the response, but further research and interviews with those responsible for managing public information are required.

Conclusion

The issue of foreign and domestic-extremist information operations potentially interfering with domestic response operations is a new normal for emergency response. The response to the East Palestine, Ohio, derailment showed the reach of foreign information operations, and the incident was used to advance domestic-extremist agendas. The impact of foreign and domestic-extremist information operations and strategies for prevention and management are areas

that need additional future research. As the Supreme Court continues to shape the legal framework under existing law, with two cases decided and one pending, legislative changes are also being considered for the potential regulation of social media platforms. As a result, the legal framework for the future is uncertain.

Endnotes

1. Camille Francois and Herb Lin, "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot," *Journal of Cyber Policy* 6, no. 1 (2021): 9–30.

2. Andrew R. N. Ross et al., "Russian Meddling in U.S. Elections: How News of Disinformation's Impact Can Affect Trust in Electoral Outcomes and Satisfaction with Democracy," *Mass Communication and Society* 25, no. 6 (2022): 786–811.

3. Marek N. Posard and Jessica Jensen, "A Foreign Government, Oprah, and Fires in Maui: The Impact of Misinformation on Community Resiliency," RAND Corporation, February 23, 2024, https://www.rand.org/pubs/commentary/2024/02/a-foreign-government-oprah-and-fires-in-maui-the-impact.html.

4. US Department of Defense (DoD), *DOD Dictionary of Military and Associated Terms* (DoD, November 2021), 104.

5. US Department of Homeland Security (DHS), *Homeland Threat Assessment 2024* (DHS, 2024).

6. DHS, *Homeland Threat Assessment 2024*, 6.

7. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (ODNI, February 5, 2024).

8. ODNI, *Annual Threat Assessment*, 12.

9. Foreign Malign Influence Center, 50 U.S.C. § 3059 (2023).

10. ODNI, *Annual Threat Assessment*, 31.

11. DHS, *Homeland Threat Assessment*, 1.

12. DHS, *Homeland Threat Assessment*, 7.

13. DHS, *Homeland Threat Assessment*, 6.

14. "Norfolk Southern Railway Derailment and Hazardous Materials Release," National Transportation Safety Board (NTSB), n.d., accessed on January 31, 2024, https://www.ntsb.gov/investigations/Pages/RRD23MR005.aspx.

15. "Norfolk Southern Railway."

16. Michael DeWine, "East Palestine Update: Evacuation Area Extended, Controlled Release of Rail Car Contents Planned for 3:30 p.m.," GovDelivery, February 6, 2023, https://content.govdelivery.com/accounts/OHIOGOVERNOR/bulletins/3473403?reqfrom=share.

17. DeWine, "East Palestine Update."

18. Jason El-Zein, *Norfolk Southern East Palestine Train Derailment General Notice Letter* (Environmental Protection Agency, February 10, 2023).

19. The White House, *Fact Sheet: One Year after Train Derailment, Biden-Harris Administration Continues to Support People in East Palestine, Ohio and Nearby Communities and Hold Norfolk Southern Accountable* (The White House, January 31, 2024).

20. "Remarks by President Biden on Supporting the Community in East Palestine, Ohio," The White House, February 16, 2024, https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/02/16/remarks-by-president-biden-on-supporting-the-community-in-east-palestine-ohio-east-palestine-oh/.

21. "East Palestine Train Derailment," Ohio Emergency Management Agency, n.d., accessed on January 10, 2025, https://ema.ohio.gov/media-publications/east-palestine-derailment-info.

22. "Investigative Hearing: Norfolk Southern Railway Train Derailment with Subsequent Hazardous Material Release and Fires," NTSB, n.d., accessed on January 10, 2025, https://www.ntsb.gov/news/events/Pages/East-Palestine-Hearing-Event.aspx.

23. "Failed Wheel Bearing Caused Norfolk Southern Train Derailment in East Palestine, Ohio," NTSB, June 25, 2024, https://www.ntsb.gov/news/press-releases/Pages/NR20240625.aspx.

24. Ty Roush, "Pro-Russia Twitter Trolls Stoked Fears about Ohio Derailment, Analysis Shows," *Forbes*, March 18, 2023, https://www.forbes.com/sites/tylerroush/2023/03/18/pro-russia-twitter-trolls-stoked-fears-about-ohio-derailment-analysis-shows/?sh=6567367d616b.

25. David Klepper, "Pro-Moscow Voices Tried to Steer Ohio Train Disaster Debate," Associated Press, March 18, 2023, https://apnews.com/article/ohio-train-derailment-russia-disinformation-twitter-musk-49af27699727d6f4157a5d6d5f35819b; and Chris Mueller and Eleanor McCrary, "Ohio Train Derailment Fact Check: What's True and What's False?," *USA Today*, updated February 20, 2023, https://www.usatoday.com/story/news/factcheck/2023/02/16/east-palestine-ohio-train-derailment-fact-check/11263859002/.

26. Roush, "Pro-Russia Twitter Trolls."

27. Niala Boodhoo, "FEMA Chief 'Very Concerned' about Disinformation from U.S. Adversaries after Disasters," Axios, December 4, 2023, https://www.axios.com/2023/12/04/disinformation-misinformation-russia-china-cop28-fema.

28. "Extremists Co-Opt Norfolk Southern Train Derailment in East Palestine, Ohio," Anti-Defamation League, March 6, 2023, https://www.adl.org/resources/blog/extremists-co-opt-norfolk-southern-train-derailment-east-palestine-ohio.

29. "Extremists Co-Opt Norfolk."

30. "Extremists Co-Opt Norfolk."

31. Valerie C. Brannon, *False Speech and the First Amendment: Constitutional Limits on Regulating Misinformation*, Congressional Research Service (CRS) Report IF12180 (CRS, August 1, 2022), 1.

32. Dawn Carla Nunziato, "Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation," *First Amendment Law Review* 19, no. 1 (2020).

33. Brannon, *False Speech*.

34. Caio C. V. Machado and Thaís Helena Aguiar, "Emerging Regulations on Content Moderation and Misinformation Policies of Online Media Platforms: Accommodating the Duty of Care into Intermediary Liability Models," *Business and Human Rights Journal* 8, no. 2 (2023): 244–51.

35. Nina Brown and Jonathan Peters, "Say This, Not That: Government Regulation and Control of Social Media," *Syracuse Law Review* 68 (June 2018): 521–42.

36. Deborah Fisher, "Twitter v. Taamneh," Free Speech Center at Middle Tennessee State University, updated July 2, 2024, https://firstamendment.mtsu.edu/article/twitter-v-taamneh/.

37. Fisher, "Twitter v. Taamneh."

38. "Murthy v. Missouri," Oyez, n.d., accessed on January 10, 2025, https://www.oyez.org/cases/2023/23-411.

39. US Supreme Court, *23-411 Murthy v. Missouri* (US Supreme Court, October 20, 2023).

40. Kristen E. Busch, *Social Media Algorithms: Content Recommendation, Moderation, and Congressional Considerations*, CRS Report IF12462 (CRS, July 27, 2023), 2.

41. Busch, *Social Media Algorithms*.

42. Busch, *Social Media Algorithms*, 2.

43. Luke J. Matthews et al., "Protecting Free Speech Compels Some Form of Social Media Regulation," RAND Corporation, October 20, 2023, https://www.rand.org/pubs/commentary/2023/10/protecting-free-speech-compels-some-form-of-social.html.

44. Arthur S. Hayes et al., "Shifting Roles, Enduring Values: The Credible Journalist in a Digital Age," *Journal of Mass Media Ethics* 22, no. 4 (2007): 262–79.

45. Mason Walker, "U.S. Newsroom Employment Has Fallen 26% since 2008," Pew Research Center, July 13, 2021, https://www.pewresearch.org/short-reads/2021/07/13/u-s-newsroom-employment-has-fallen-26-since-2008/.

46. "Occupational Outlook Handbook," US Bureau of Labor Statistics, n.d., accessed on January 31, 2024, https://www.bls.gov/ooh/media-and-communication/reporters-correspondents-and-broadcast-news-analysts.htm.

47. Amy Mitchell et al., "Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable," Pew Research Center, July 30, 2020, https://www.pewresearch.org/journalism/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeable/.

48. Mitchell et al., "News on Social Media."

49. Rebecca Leppert and Katerina Eva Matsa, "More Americans—Especially Young Adults—Are Regularly Getting News on TikTok," Pew Research Center, September 17, 2024, https://www.pewresearch.org/short-reads/2023/11/15/more-americans-are-getting-news-on-tiktok-bucking-the-trend-seen-on-most-other-social-media-sites/.

50. Leppert and Matsa, "More Americans."

51. Cailey Gleeson, "These 39 States Already Ban TikTok from Government Devices," *Forbes*, March 12, 2024, https://www.forbes.com/sites/caileygleeson/2024/03/12/these-39-states-already-ban-tiktok-from-government-devices/?sh=52baa1ac6705.

52. Matthews et al., "Protecting Free Speech."

53. Paul Machete and Marita Turpin, "The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review," in *Responsible Design, Implementation and Use of Information and Communication Technology*, ed. Marié Hattingh et al. (Springer, 2020).

54. M. Mitchell Waldrop, "How to Mitigate Misinformation," *Proceedings of the National Academy of Sciences* 120, no. 36 (2023).

55. Soroush Vosoughi et al., "The Spread of True and False News Online," *Science* 359, no. 6380 (March 2018): 1146–51.

56. Gizem Ceylan et al., "Sharing of Misinformation Is Habitual, Not Just Lazy or Biased," *Proceedings of the National Academy of Sciences* 120, no. 4 (January 2023).

57. DHS, *Countering False Information on Social Media in Disasters and Emergencies* (DHS, March 2018).

58. Ramian Fathi and Frank Fiedrich, "Social Media Analytics by Virtual Operations Support Teams in Disaster Management: Situational Awareness and Actionable Information for Decision-Makers," *Frontiers in Earth Science* 10 (September 2022).

59. DHS, *Countering False Information*.

60. DHS, *Countering False Information*.

61. DHS, *Countering False Information*.

62. Jennifer Homendy (@JenniferHomendy), "THREAD on East Palestine derailment: First, a message to the community . . . then a plea to those spreading misinformation," X, February 16, 2023, https://twitter.com/JenniferHomendy/status/1626379352215547906.

Bibliography

Anti-Defamation League. "Extremists Co-Opt Norfolk Southern Train Derailment in East Palestine, Ohio." March 6, 2023. https://www.adl.org/resources/blog/extremists-co-opt-norfolk-southern-train-derailment-east-palestine-ohio.

Brannon, Valerie C. *False Speech and the First Amendment: Constitutional Limits on Regulating Misinformation*. Congressional Research Service Report IF12180. Congressional Research Service, 2022.

Brown, Nina I. and Jonathan Peters. "Say This, Not That: Government Regulation and Control of Social Media." *Syracuse Law Review* 68 (2018): 521–42.

Busch, Kristen E. *Social Media Algorithms: Content Recommendation, Moderation, and Congressional Considerations*. Congressional Research Service Report IF12462. Congressional Research Service, 2023.

Ceylan, Gizem, Ian Anderson, and Wendy Wood. "Sharing of Misinformation Is Habitual, Not Just Lazy or Biased." *Proceedings of the National Academy of Sciences* 120, no. 4 (2023).

DeWine, Michael. "East Palestine Update: Evacuation Area Extended, Controlled Release of Rail Car Contents Planned for 3:30 p.m." GovDelivery, February 6, 2023. https://content.govdelivery.com/accounts/OHIOGOVERNOR/bulletins/3473403?reqfrom=share.

DeWine, Michael. "East Palestine Update: Residents Can Safety Return Home." GovDelivery, February 6, 2023. https://content.govdelivery.com/accounts/OHIOGOVERNOR/bulletins/347a700?reqfrom=share.

El-Zein, Jason. *Norfolk Southern East Palestine Train Derailment General Notice Letter*. Environmental Protection Agency, February 10, 2023.

Fathi, Ramian and Frank Fiedrich. "Social Media Analytics by Virtual Operations Support Teams in Disaster Management: Situational Awareness and Actionable Information for Decision-Makers." *Frontiers in Earth Science* 10 (September 2022).

Fisher, Deborah. "Twitter v. Taamneh." Free Speech Center at Middle Tennessee State University, updated July 2, 2024. https://firstamendment.mtsu.edu/article/twitter-v-taamneh/.

Francois, Camille and Herb Lin. "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot." *Journal of Cyber Policy* 6, no. 1 (2021): 9–30.

Gleeson, Cailey. "These 39 States Already Ban TikTok from Government Devices." *Forbes*, March 12, 2024. https://www.forbes.com/sites/caileygleeson/2024/03/12/these-39-states-already-ban-tiktok-from-government-devices/?sh=52baa1ac6705.

Hayes, Arthur S., Jane B. Singer, and Jerry Ceppos. "Shifting Roles, Enduring Values: The Credible Journalist in a Digital Age." *Journal of Mass Media Ethics* 22, no. 4 (2007): 262–79.

Klepper, David. "Pro-Moscow Voices Tried to Steer Ohio Train Disaster Debate." Associated Press, March 18, 2023. https://apnews.com/article/ohio-train-derailment-russia-disinformation-twitter-musk-49af27699727d6f4157a5d6d5f35819b.

Machado, Caio C. V. and Thaís Helena Aguiar. "Emerging Regulations on Content Moderation and Misinformation Policies of Online Media Platforms: Accommodating the Duty of Care into Intermediary Liability Models." *Business and Human Rights Journal* 8, no. 2 (2023): 244–51.

Machete, Paul and Marita Turpin. "The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review." In *Responsible Design, Implementation and Use of Information and Communication Technology*, edited by Marié Hattingh et al. Springer, 2020.

Matthews, Luke J., Heather J. Williams, and Alexandra T. Evans. "Protecting Free Speech Compels Some Form of Social Media Regulation." RAND Corporation, October 20, 2023. https://www.rand.org/pubs/commentary/2023/10/protecting-free-speech-compels-some-form-of-social.html.

Mitchell, Amy, Mark Jurkowitz, J. Baxter Oliphant, and Elisa Shearer. "Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable." Pew Research Center, July 30, 2020. https://www.pewresearch.org/journalism/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeable/.

Mueller, Chris and Eleanor McCrary. "Ohio Train Derailment Fact Check: What's True and What's False?" *USA Today*, updated February 20, 2023. https://www.usatoday.com/story/news/factcheck/2023/02/16/east-palestine-ohio-train-derailment-fact-check/11263859002/.

National Transportation Safety Board. "Failed Wheel Bearing Caused Norfolk Southern Train Derailment in East Palestine, Ohio." Accessed September 9, 2024. https://www.ntsb.gov/news/press-releases/Pages/NR20240625.aspx.

National Transportation Safety Board. "Norfolk Southern Railway Derailment and Hazardous Materials Release." Accessed April 24, 2024. https://www.ntsb.gov/investigations/Pages/RRD23MR005.aspx.

Nunziato, Dawn Carla. "Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation." *First Amendment Law Review* 19, no. 1 (2020).

Office of the Director of National Intelligence. *2024 Annual Threat Assessment of the Intelligence Community*. Office of the Director of National Intelligence, 2024.

Posard, Marek N. and Jessica Jensen. "A Foreign Government, Oprah, and Fires in Maui: The Impact of Misinformation on Community Resiliency." *Domestic Preparedness Journal*, February 21, 2024. https://www.domesticpreparedness.com/articles/a-foreign-government-oprah-and-fires-in-maui.

Ross, Andrew R. N., Cristian Vaccari, and Andrew Chadwick. "Russian Meddling in U.S. Elections: How News of Disinformation's Impact Can Affect Trust in Electoral Outcomes and Satisfaction with Democracy." *Mass Communication and Society* 25, no. 6 (2022): 786–811.

Roush, Ty. "Pro-Russia Twitter Trolls Stoked Fears About Ohio Derailment, Analysis Shows." *Forbes*, March 18, 2023. https://www.forbes.com/sites/tylerroush/2023/03/18/pro-russia-twitter-trolls-stoked-fears-about-ohio-derailment-analysis-shows/?sh=6567367d616b.

US Bureau of Labor Statistics. "Occupational Outlook Handbook." Updated August 29, 2024. https://www.bls.gov/ooh/media-and-communication/reporters-correspondents-and-broadcast-news-analysts.htm.

US Department of Defense. DOD Dictionary of Military and Associated Terms. Department of Defense, 2021.

US Department of Homeland Security. *Countering False Information on Social Media in Disasters and Emergencies*. Department of Homeland Security, 2018.

US Department of Homeland Security. *Homeland Threat Assessment 2024*. Department of Homeland Security, 2024.

US Supreme Court. *23-411 Murthy v. Missouri*. US Supreme Court, October 20, 2023.

Vosoughi, Souroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (March 2018): 1146–51.

Waldrop, M. Mitchell. "How to Mitigate Misinformation." *Proceedings of the National Academy of Sciences* 120, no. 36 (2023).

Walker, Mason. "U.S. Newsroom Employment Has Fallen 26% Since 2008." Pew Research Center, July 13, 2021. https://www.pewresearch.org/short-reads/2021/07/13/u-s-newsroom-employment-has-fallen-26-since-2008/.

White House. *Fact Sheet: One Year After Train Derailment, Biden-Harris Administration Continues to Support People in East Palestine, Ohio and Nearby Communities and Hold Norfolk Southern Accountable*. White House, January 31, 2024.

— 2 —

Cognitive Warfare

Michael Roi, PhD

ABSTRACT: Since no commonly accepted definition of cognitive defense exists, this chapter focuses on cognitive warfare. The chapter uses a working definition of cognitive warfare that draws on NATO's work on the concept and will briefly examine Russian and Chinese thinking about cognitive warfare as well. The conclusion offers solutions regarding what must be done to defend against Russian and Chinese use of cognitive warfare.

Introduction

A quick Internet search reveals no widely or commonly accepted definition of cognitive defense. In contrast, cognitive warfare has been used more in the last five years. This chapter thus focuses on cognitive warfare because the latter term enjoys wider usage, and because a reasonable first step seems to be understanding the more significant problem space of cognitive warfare before designing specific solutions for cognitive defense. The chapter will use a working definition of cognitive warfare that draws on NATO's understanding of the concept. This definition will be followed by a brief examination of Russian and Chinese thinking about cognitive warfare. The chapter concludes by discussing what must be done to defend against Russian and Chinese use of cognitive warfare.

For the past few years, NATO has been exploring the concept of cognitive warfare. The alliance defines cognitive warfare thus.

> The activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group

> cognitions to gain an advantage . . . . Cognitive Warfare integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other Instruments of Power, can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary.[1]

According to NATO, cognitive warfare harnesses new technology and recent theoretical insights from fields like cognitive psychology.[2] Cognitive warfare integrates cyber and artificial intelligence developments with information, psychological, and social-engineering capabilities.[3] As such, social media has become a critical battlefront in warfare.

Cognitive warfare should be seen as a struggle to shape, influence, and potentially change the thinking of an individual or a group. This term is sometimes used interchangeably with terms like information warfare. As NATO's definition makes clear, one should not think about cognitive warfare as somehow distinct from kinetic or physical actions. One must avoid this simplistic binary delineation. Actions in the cognitive sense and physical developments (such as events on the battlefield) are not necessarily independent and, in certain circumstances, can be mutually reinforcing. An obvious point worth restating is physical developments on the battlefield can influence thinking both on the front lines and beyond, especially when accompanied by deliberate information efforts to promote a particular understanding of what is happening and what the physical developments mean.

In cognitive warfare, an individual's or a group's cognition is now the target. Cognitive warfare involves more than controlling the flow of information. Instead, it aims to manipulate, influence, and control how people react to information. Cognitive warfare can aggravate domestic tensions, exacerbating societal polarization and radicalization. Advances in cognitive psychology and information technology enable actors to target individuals' perceptions and, ultimately, one's will. Perhaps the best analytical approach is to consider cognitive warfare an emerging, not fully developed warfighting idea, drawing on some older principles and thinking on military affairs. Although the term may be new, shaping an adversary's thinking is not. Earlier theorists like Sun Tzu and Carl von Clausewitz emphasized the importance of will and morale in war (see the paper by George Schwartz in this collection of conference papers). The concept of cognitive warfare may be embryonic; nevertheless, three broad elements are associated with the concept, as discussed in a recent article in the journal *Proceedings*. First is a deliberate intent to influence the thinking of specific individuals and groups on political, social, and related issues. Second, human cognition or understanding is directly targeted based on theories of how people perceive, process, and share information. Third, cognitive

warfare uses psychology and advanced information technologies or tools, including the increasing use of artificial intelligence, to target specific individuals or groups precisely. Cognitive warfare can be seen as precision-guided psychological or information campaigns.[4] Much of the research and analytic focus has been, not surprisingly, on understanding Russian and Chinese approaches to cognitive warfare. Let us take a closer look at these approaches, starting with Russia.

Russian Cognitive-Warfare Theory

Russian information-warfare or cognitive-warfare theories originated in the Cold War with the Soviet reflexive-control theory. A detailed discussion of reflexive control lies beyond the scope of this chapter. For interested readers, several recent articles have provided a more in-depth examination of reflexive control.[5] Timothy Thomas did much of the early pioneering work on Russian theories of reflexive control.[6] For the past decade, Keir Giles of Chatham House has done excellent work on the Russian approach to reflexive control and information warfare.[7] In a nutshell, reflexive control draws insights from psychology and game theory to control an opponent's actions by manipulating the information environment. Reflexive control causes an opponent to make decisions that favor Russia, often to the opponent's detriment. Russian leaders apply information-warfare practices against their people; the populations of neighboring countries; and beyond, targeting citizens across NATO, including our people here in the United States and Canada.

The Russia-Ukraine War has given us a front-row seat to the Russian approach to cognitive and information warfare, demonstrating how Moscow customizes information to specific audiences. At home, the Kremlin continues to frame and justify its long-term military effort in Ukraine as part of an existential geopolitical confrontation with the West and a necessary struggle against "Nazism."[8] Russian President Vladimir Putin and other Russian leaders repeatedly draw parallels to previous Russian victories in World War II, known in Russia as the Great Patriotic War, to defeat Nazi Germany.[9] Isolating the Russian people from outside information is a crucial enabler of Moscow's information campaign. The Kremlin has put substantial and long-term effort into ensuring a controlled information space without tolerance for unsanctioned viewpoints.

Moscow also tailors information to specific groups outside Russia. As highlighted in a recent Institute for the Study of War report, Russia is making efforts to drive wedges between Ukraine and some of its Western neighbors.[10] This analysis shows Russia is seizing on and fueling neo-imperialist and right-wing nationalist sentiments across Europe. Right-wing parties in Hungary

and Romania, for example, have been calling for the partition of Ukraine and the so-called reintegration of Ukrainian territory they argue historically belongs to their countries. Russian sources have amplified and repeatedly spread right-wing Hungarian and Romanian messages. The Institute for the Study of War adds various Russian politicians have for some years proposed the idea of a "partitioned Ukraine," including just before the full-scale invasion in February 2022.[11] Putin and other senior Russian officials recently returned to the narrative of a partitioned Ukraine in December 2023 by claiming Ukraine's territory remains contested, citing historical "territorial disputes" with Poland, Romania, and Hungary.[12] Russian disinformation efforts lean heavily on derogatory stereotypes of Ukrainians and deeply flawed readings of the history of Ukraine, and these efforts have included outright Russian imperial declarations Ukrainians are not a separate people but rather "Little Russians."[13] Globally, Russia continues to exploit opportunities to sow political and social divisions in the societies of Western nations opposed to Russia's aggression against Ukraine. An apposite example of efforts to sow political disunity through Russian propaganda and disinformation is evident in the US Department of Justice's indictment of two Russian nationals, both employees of the Russian state-controlled RT, for "a $10 million scheme to create and distribute content to U.S. audiences with hidden Russian government messaging."[14]

Chinese Cognitive-Warfare Theory

Like the Kremlin, Chinese leaders in Beijing have been aggressively pursuing a cognitive-warfare campaign against multiple audiences. Beijing targets its people and the citizens of Hong Kong, Taiwan, and other nations in the Indo-Pacific.[15] Globally, Beijing seeks to weaken the appeal of democracies and to denigrate the United States. Josh Baughman and Peter W. Singer have looked closely at Chinese writings on cognitive warfare and the use of information. Writing in Defense One, Baughman and Singer demonstrate China's social media attacks are part of a cognitive-warfare campaign. The authors contend, "Chinese government and military writings say cognitive operations aim to 'capture the mind' of one's foes, shaping an adversary's thoughts and perceptions and consequently their decisions and actions."[16] According to Chinese military writings, the People's Liberation Army puts cognitive warfare on par with the other domains of warfare like land, air, sea, and space—and believes cognitive warfare is crucial to victory.[17] Beijing clearly understands the power of social media to shape narratives and cognition over events and actions.[18] In effect, social media platforms are viewed as the main battlefield of the cognitive-warfare fight. As Baughman and Singer point out, "When a typical user spends 2.5 hours a day on social media—

36 full days out of the year, 5.5 years in an average lifespan—it is perhaps no surprise that the Chinese Communist Party believes it can, over time, shape and even control the cognition of individuals and whole societies."[19]

Chinese officials use Chinese and foreign-language platforms, including widespread automated accounts (bots), to shape narratives and cognition over events and actions. The Chinese use of social media in promoting Beijing's view of the Xinjiang region and the treatment of Uyghurs there and elsewhere provides a case in point. As Albert Zhang and Tilla Hoja point out:

> The Chinese Communist Party is using social media and disinformation campaigns to project its preferred narratives about Xinjiang and influence unwitting audiences around the globe. Instead of improving its treatment of Uyghurs and other Turkic minorities, the CCP is responding to critiques of its human rights record by coordinating its state propaganda apparatus, security agencies, and public relations industry to influence and even silence governments, businesses and civil society at home and abroad.[20]

Social media was undoubtedly a battleground during the 2019 democracy protests in Hong Kong.[21] Chinese mainland accounts aggressively used social media, notably WeChat, Weibo, Facebook, X, and YouTube, to attempt to undermine the protests. X and Facebook turned off hundreds if not thousands of accounts linked to mainland China.[22] Not all the Chinese government's attempts to use social media were sophisticated and successful, especially after journalists and social media platforms exposed the Chinese Communist Party's covert and coordinated social media campaign.[23] In many ways, China lost the social media battle over Hong Kong and certainly beyond, in places like Taiwan, where the Taiwanese reacted negatively to Beijing's de facto rejection of the two-systems approach in Hong Kong.[24] Beijing may have lost the social media battle but China still prevailed in imposing greater political and physical control over Hong Kong. Physical means still matter, and information operations and cognitive warfare alone can only achieve limited results. Like Russia, China is also engaged in a significant information campaign to undermine democracies globally while promoting autocracies, which brings us back to the focus of the symposium: the defense of our homelands.

Threat to Our Homelands: How to Respond

Moscow and Beijing target our societies. They seek to erode our prosperity and undermine our political independence. Russia and China's efforts go well beyond targeting our governments; the efforts include the private sector, nongovernmental organizations, academia, and our citizens. In essence, Russian and Chinese targeting is a whole-of-society or whole-of-nation threat. Through efforts to interfere with our political processes, sow discord and exacerbate existing partisan divisions, and sap our confidence in democracy, Russia and China seek to diminish the appeal of democracy, undermine the rules-based international order, and promote their form of autocratic governance. Using espionage and cyberhacking, these adversaries attempt to steal vital and valuable intellectual property and crucial scientific research, gradually eroding the foundations of our countries' economic well-being. Chinese strategists believe strategic objectives can be achieved through direct action against enemy cognition. As the former deputy chief of staff of the People's Liberation Army insists, "Those who gain the upper hand in developing new-generation artificial intelligence technologies will be able to control the lifeline of national security: human cognition."[25] What should we do to meet this challenge? What is our cognitive defense against the cognitive-warfare threat?

Collectively, governments at all levels, in partnership with businesses and citizens, must strengthen the resilience of our political institutions and citizenry and protect our democratic processes. Governments must also be prepared to seize the initiative, taking the fight to our adversaries. We must defeat or counter adversarial cognitive attacks, conducting our campaign to defend our democracies and make the world increasingly unreceptive to the appeal of autocracy. Cognitive defense requires our leaders to possess a strong defensive-sensing capability to detect and protect us from cognitive and information attacks. Effective defense requires the awareness a cognitive-warfare campaign is underway. We must understand the origins, motivations, objectives, and people or organizations behind cognitive-warfare campaigns. We must develop the ability to observe and orient a cognitive and resilient defensive posture. As generative artificial intelligence becomes increasingly sophisticated, the scale of this challenge will likely grow.

We can learn from the Finnish example of "comprehensive security."[26] The Finnish government, along with its citizens, pursues a comprehensive-security strategy where everyone is, to some degree, a security actor, and each shares a part in providing for the defense and security of Finnish society. Empowering and enabling citizens to play a role in ensuring Finnish security is critical to promoting societal resilience.[27] The Finnish approach to preparedness,

backed by the active engagement of senior political figures and government officials, consists of

> 1. frank public discussions about threats and risks to Finland and its citizens;
>
> 2. ongoing public outreach by security services, including to secondary schools and the private sector;
>
> 3. defense courses offered nationwide, providing military personnel and civilians with information about Finland's foreign, security, and defense policy, including material on resilience, national preparedness, national legislation, and decision-making processes; and
>
> 4. continual monitoring, assessment, and adjustment of security measures by the central government in relation to routine reviews of the threat environment.

All the elements of Finnish comprehensive security contribute to a culture of security awareness, helping to build a shared understanding of threats and to promote psychological resilience among Finnish citizens. Comprehensive security provides the foundation for national preparedness and underpins supply chain and industrial strategies, ensuring Finland is better prepared for emergencies and crises. The Finnish government perceives national and individual resilience and preparedness as necessary elements of deterrence. Finland's comprehensive-security strategy reflects its history of complex relations with its Russian neighbor. The threat in Finland is palpable and persistent. But as the above discussion of cognitive warfare illustrates, distance provides no sanctuary. We can learn from the Finns: We need to be frank with our citizens about threats and look at ways to include our citizens in the cognitive defense of their homeland.

Endnotes

1. "Cognitive Warfare: Strengthening and Defending the Mind," NATO Allied Command Transformation, April 5, 2023, https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

2. "Cognitive Warfare."

3. "Cognitive Warfare."

4. Andrew MacDonald and Ryan Ratcliffe, "Cognitive Warfare: Maneuvering in the Human Dimension," *Proceedings,* April 2023, https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension.

5. John Merriam, "One Move Ahead—Diagnosing and Countering Russian Reflexive Control," *Journal of Slavic Military Studies* 36, no. 1 (2023): 1–27; and Maria W. R. de Goeij, "Reflexive Control: Influencing Strategic Behavior," *Parameters* 53, no. 4 (Winter 2023–24): 97–108. See also the monograph by Antti Vasara, *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy,* Finnish Defense Studies no. 22 (Finnish National Defence University, 2020).

6. Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56.

7. Keir Giles, *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine* (Chatham House, December 2023); Keir Giles, *Handbook of Russian Information Warfare*, Fellowship Monograph no. 9 (NATO Defense College, November 2016); and Keir Giles et al., *Russian Reflexive Control*, Contract Report no. DRDC-RDDC-2018-C182 (Defence Research and Development Canada, October 2018).

8. Tom Porter, "Putin Accuses the West of Creating Nazis While Comparing the War in Ukraine to WWII, in What Experts Are Calling a Perversion of History," *Business Insider*, May 9, 2023, https://www.businessinsider.com/victory-day-speech-putin-blames-west-creating-cult-nazism-russia2023-5.

9. Porter, "Putin Accuses the West."

10. Angelica Evans et al., "Russian Offensive Campaign Assessment, January 29, 2024," Institute for the Study of War, January 29, 2024, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-29-2024.

11. Evans et al., "Russian Offensive Campaign Assessment."

12. Evans et al., "Russian Offensive Campaign Assessment."

13. Taras Kuzio, "Imperial Nationalism as the Driver Behind Russia's Invasion of Ukraine," *Nations and Nationalism* 29, no. 1 (January 2023): 30–38. Yale University historian Timothy Snyder has widely debunked Putin's use of history. See Snyder's essay on Putin's interview with Tucker Carlson: Timothy Snyder, "Putin's Genocidal Myth," *Thinking About . . .* (blog), February 11, 2024, https://snyder.substack.com/p/putins-genocidal-myth.

14. US Department of Justice, "Two RT Employees Indicted for Covertly Funding and Directing U.S. Company That Published Thousands of Videos in Furtherance of Russian Interests," press release no. 24-1094, September 4, 2024, https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands.

15. For a detailed discussion of the Chinese cognitive warfare campaign against Taiwan, see Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," *Journal of Global Security Studies* 7, no. 4 (December 2022): 1–18.

16. Josh Baughman and Peter W. Singer, "China's Social-Media Attacks Are Part of a Larger 'Cognitive Warfare' Campaign," Defense One, October 17, 2023, https://www.defenseone.com/ideas/2023/10/chinas-social-media-attacks-are-part-larger-cognitive-warfare-campaign/391255/.

17. For a discussion of the growing importance to Chinese military thinkers of the mind as a domain in warfare, see Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, Report no. RR-A853-1 (RAND Corporation, 2023), 21–35.

18. Scott W. Harold et al., *Chinese Disinformation Efforts on Social Media*, Report no. RR-4373/3-AF (RAND Corporation, 2021), 11–31.

19. Baughman and Singer, "China's Social-Media Attacks."

20. Albert Zhang and Tilla Hoja, "China's Information Operations Are Silencing and Influencing Global Audiences on Xinjiang," *Strategist* (blog), July 20, 2022, https://www.aspistrategist.org.au/chinas-information-operations-are-silencing-and-influencing-global-audiences-on-xinjiang/.

21. Grace Shao, "Social Media Has Become a Battleground in Hong Kong's Protests," *CNBC*, updated August 16, 2019, https://www.cnbc.com/2019/08/16/social-media-has-become-a-battleground-in-hong-kongs-protests.html; and Emily Stewart, "How China Used Facebook, Twitter, and YouTube to Spread Disinformation About the Hong Kong Protests," *Vox*, August 23, 2019, https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media.

22. Harold et al., *Chinese Disinformation Efforts*, 33–34; and Stewart, "How China Used Facebook."

23. Beauchamp-Mustafaga, *Next-Generation Psychological Warfare*, 114; and John Dotson, "Chinese Covert Social Media Propaganda and Disinformation Related to Hong Kong," *China Brief* 19, no. 16 (September 2019): 1–7.

24. China's heavy-handed approach to suppressing the democratic and human rights of the people in Hong Kong has promoted sympathies and spurred supportive actions in Taiwan. See Timothy Rich and Isabel Eliassen, "A Political Analysis of Taiwanese Perceptions of Hong Kong Protests," Global Taiwan Institute, September 23, 2020, https://globaltaiwan.org/2020/09/a-political-analysis-of-taiwanese-perceptions-of-hong-kong-protests/.

25. Koichiro Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," War on the Rocks, July 22, 2022, https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/.

26. "Concept of Comprehensive Security—Building National Resilience in Finland," Security Committee, Ministry of Defense of Finland, n.d., accessed on January 7, 2025, https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/.

27. "Concept of Comprehensive Security."

Bibliography

Baughman, Josh and Peter W. Singer. "China's Social-Media Attacks Are Part of a Larger 'Cognitive Warfare' Campaign." Defense One, October 17, 2023. https://www.defenseone.com/ideas/2023/10/chinas-social-media-attacks-are-part-larger-cognitive-warfare-campaign/391255/.

Beauchamp-Mustafaga, Nathan. *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*. Report no. RR-A853-1. RAND Corporation, 2023.

de Goeij, Maria W. R. "Reflexive Control: Influencing Strategic Behavior." *Parameters* 53, no. 4 (Winter 2023–24): 97–108.

Dotson, John. "Chinese Covert Social Media Propaganda and Disinformation Related to Hong Kong." *China Brief* 19, no. 16 (September 2019): 1–7.

Evans, Angelica, Riley Bailey, and Nicole Wolkoc, et al. "Russian Offensive Campaign Assessment, January 29, 2024." Institute for the Study of War, January 29, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-29-2024.

Giles, Keir. *Handbook of Russian Information Warfare*. Fellowship Monograph no. 9. NATO Defense College, 2016.

Giles, Keir. *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*. Chatham House, 2023.

Giles, Keir, James Sherr, and Anthony Seaboyer. *Russian Reflexive Control*. Contract Report no. DRDC-RDDC-2018-C182. Defence Research and Development Canada, 2018.

Harold, Scott W. et al. *Chinese Disinformation Efforts on Social Media*. Report no. RR-4373/3-AF. RAND Corporation, 2021.

Hung, Tzu-Chieh and Tzu-Wei Hung. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." *Journal of Global Security Studies* 7, no. 4 (2020): 1–18.

Kuzio, Taras. "Imperial Nationalism as the Driver Behind Russia's Invasion of Ukraine." *Nations and Nationalism* 29, no. 1 (2023): 30–38.

MacDonald, Andrew and Ryan Ratcliffe. "Cognitive Warfare: Maneuvering in the Human Dimension." *Proceedings*, April 2023. https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension.

Merriam, John. "One Move Ahead—Diagnosing and Countering Russian Reflexive Control." *Journal of Slavic Military Studies* 36, no. 1 (2023): 1–27.

NATO Allied Command Transformation. "Cognitive Warfare: Strengthening and Defending the Mind." April 5, 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

Rich, Timothy and Isabel Eliassen. "A Political Analysis of Taiwanese Perceptions of Hong Kong Protests." Global Taiwan Institute, September 23, 2020. https://globaltaiwan.org/2020/09/a-political-analysis-of-taiwanese-perceptions-of-hong-kong-protests/.

Security Committee, Ministry of Defense of Finland. "Concept of Comprehensive Security—Building National Resilience in Finland." Accessed January 7, 2025. https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/.

Shao, Grace. "Social Media Has Become a Battleground in Hong Kong's Protests." *CNBC*, updated August 16, 2019. https://www.cnbc.com/2019/08/16/social-media-has-become-a-battleground-in-hong-kongs-protests.html.

Snyder, Timothy. "Putin's Genocidal Myth." *Thinking About . . .* (blog), February 14, 2024. https://snyder.substack.com/p/putins-genocidal-myth.

Stewart, Emily. "How China Used Facebook, Twitter, and YouTube to Spread Disinformation About the Hong Kong Protests." *Vox*, August 23, 2019. https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media.

Takagi, Koichiro. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." War on the Rocks, July 22, 2022. https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/.

Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56.

Vasara, Antti. *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy.* Finnish Defense Studies no. 22. Finnish National Defense University, 2020.

Zhang, Albert and Tilla Hoja. "China's Information Operations Are Silencing and Influencing Global Audiences on Xinjiang." *Strategist* (blog), July 20, 2022. https://www.aspistrategist.org.au/chinas-information-operations-are-silencing-and-influencing-global-audiences-on-xinjiang/.

— 3 —

Cognitive Warfare: Homeland Strong?

George M. Schwartz, EdD

ABSTRACT: Americans' minds are under attack as foreign competitors strive to weaken our national power by creating discord and mistrust. This chapter will provide context for the concept of cognitive defense and offer recommendations using an existing framework for homeland security, the National Preparedness System (NPS), and an expanded definition of resilience. The chapter will conclude with a cursory assessment of the current state of resilience in the United States in an attempt to answer the question: Is the homeland strong?

Introduction

In a December 2022 speech at the Center for Strategic and International Studies, Department of Homeland Security (DHS) Secretary Alejandro N. Mayorkas noted, "As the threats have evolved, the historical distinction between homeland security and national security challenges has blurred."[1] With our potential adversaries operating in the gray zone between war and peace, the distinction between homeland security and homeland defense has also blurred.[2]

The overlap between the two mission sets has increased as our near-peer competitors set the conditions for a future conflict through operations within our borders. For example, advanced-persistent-threat groups sponsored by the People's Republic of China are prepositioned and lurking within the networks of US critical infrastructure, poised to disrupt water and electric utilities.[3] Russia produces violent-extremist materials consumed by homegrown extremist groups that plan physical attacks on energy infrastructure to advance the groups' goal of destabilizing society to start a race war.[4]

The most pernicious actions undermining the United States's security are in the cognitive domain: the attacks on facts and truth, the campaigns to undermine our citizens' trust in democratic institutions, and the reshaping of our traditional beliefs. This chapter will provide context for the concept of cognitive defense and offer recommendations that use an existing framework for homeland security. Applying an expanded definition of resilience, the chapter will conclude with a cursory assessment of the current state of resilience in the United States.

Cognitive Warfare

Operations in the cognitive domain predominantly use cybertools, often social media, and integrate information, psychological, and social-engineering capabilities.[5] Much like psychological operations, the goal of cognitive warfare is "to alter . . . cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels."[6] Cognitive warfare differs from psychological operations in its ability to circulate and reach extreme segments of the public through the medium of cyberspace.

The North Atlantic Treaty Organization (NATO) has been at the forefront of the thought process regarding such influencing operations. The organization has characterized these deliberate activities as cognitive warfare because the term means "the weaponization of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions."[7] In the United States, foreign adversaries use low-cost cybertools to produce and disseminate disinformation and malinformation (the deliberate use of otherwise verifiable information with malicious intent) through our open networks. Artificial intelligence–enhanced products are now being used to create realistic but false media many Americans believe to be true.[8]

But the underpinnings of cognitive warfare are not new. More than 2,000 years ago, the Chinese military strategist Sun Tzu wrote in *The Art of War* about defeating armies without engaging in battle: "To subdue the enemy without fighting is the acme of skill. Thus, what is of supreme importance in war is to attack the enemy's strategy."[9] Later in chapter 5, Sun Tzu would add victory comes from sowing suspicion and confusion in other countries. Essentially, making one's enemy believe they cannot win will lead to the enemy's defeat.

Although the other great writer on military strategy, Carl von Clausewitz, did not shy away from battle, he states in *On War* that an army should aim

to disarm its enemy, to put one's foe in a position where the foe believes it cannot prevail.[10] He recognized that war is a test of wills and to defeat your enemy, overcoming the enemy's strength of will is necessary. Clausewitz defines an enemy's "power of resistance" as "the total means at his disposal and the strength of his will." And Clausewitz states, "War is thus an act of force to compel our enemy to do our will."[11]

Will is a component of Clausewitz's paradoxical trinity (see figure 3-1), which describes war as the interaction between the government, the people, and the military and its nature in the interplay of rationality, passion, and chance.[12] Will is often associated with government, such as in the question of whether the political will to pursue military action exists. For example, does the United States respond if our government establishes a redline for another nation and the other nation's actions violate that redline?

Related to will are the morale and determination of the military (which Clausewitz called spirit) and the patriotism or passion of the people, which is referred to as confidence.[13] Do the people trust their leaders to do what suits the nation, even if what suits the nation is war? Underlying will, morale, and confidence is belief.

Figure 3-1. Clausewitz's paradoxical trinity

Belief can be described as a subjective attitude a particular proposition is true.[14] For example, when faced with overwhelming odds of defeat, a military unit with high morale continues to fight and is victorious. In contrast, the numerically superior opponent that lacks determination is defeated. People can hold beliefs

without much reflection or evidence, so they can be persuaded or influenced to revise their beliefs with compelling information.

On the cognitive battlefield, "the strategic cognitive terrain is the gray zone, occupied by people who are influenced by catchy headlines and other forms of 'click bait' and form their judgments in part on that basis."[15] People can become anxious when faced with cognitive dissonance caused by inconsistencies between cognitions (that is, ideas). People will attempt to resolve the dissonance expeditiously, relying on their beliefs or biases. Over time, "receivers of . . . disinformation experience deterioration in their ability to identify fact from fiction, decaying their mental resilience, and with potential long-term impact, such as loss of trust in media."[16]

Jarrod Brook, an Australian Army officer, describes how, in an operating environment that moderates the use of violence, cognitive warfare "creates uncertainty that denies the adversary the ability to assess risk and make informed decisions based on their own interests. The three elements of the Clausewitzian trinity highlight that amplifying uncertainty and friction produces indecision and paralysis in an adversary. This indecision and friction make risk calculations uncertain and deny the ability to calibrate an adequate response."[17]

Cognitive Warfare and National Preparedness

As cybersecurity protects networks against intrusions and hacks, and counterterrorism prevents attacks by extremist groups, the homeland requires cognitive defense to protect our citizens from manipulative attacks by foreign actors. A structure for strengthening the homeland and cognitive defense already exists: the NPS. In 2011, Presidential Policy Directive-8 required the US Department of Homeland Security to create the NPS to achieve the national preparedness goal of "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[18]

The NPS has five mission areas; see figure 3-2.

1. Prevention: Prevent, avoid, or stop an imminent, threatened, or actual act of terrorism.

2. Protection: Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive.

3. Mitigation: Reduce the loss of life and property by lessening the impact of future disasters.

4. Response: Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident.

5. Recovery: Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident.

Prevention	Protection	Mitigation	Response	Recovery
The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.	The capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters.	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.	The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.	The capabilities necessary to assist communities affected by an incident to recover effectively.

Figure 3-2. The five mission areas of the NPS

With minor adaptations to some of the mission-area definitions, the NPS provides an iterative, phased approach to cognitive defense.

Prevention

Within the NPS, the prevention mission area is wholly focused on the threat of terrorism. Still, prevention could be adapted to incorporate any form of aggression on the continuum of conflict starting with the competition phase.[19] Prevention needs to begin with the national awareness cognitive warfare is being carried out, and people need to be able to recognize disinformation.[20]

In 2014, Finland started a nationwide training program, which began in kindergarten and included adults, to help its citizens recognize fake news and counter false information. A year after the program's launch, when Russian disinformation increased, the Finnish president called on every citizen to join

the effort; since the whole society had been targeted, everyone needed to take some responsibility. As a result, Finland has the highest media literacy in Europe, and as Dr. Michael Roi points out in his paper, can serve as a model for the United States and Canada.[21]

Protection

The comprehensive definition of the protection mission area needs no adaptation, and the protection function should be structured around a monitoring and alert system.[22] Multijurisdictional, interagency war rooms or operations centers could monitor disinformation and formulate response plans.[23] A monitoring and alert system could be modeled on the successful national network of fusion centers developed by the Department of Homeland Security after the September 11 attacks to counter terrorism. Under federal guidelines, state and urban fusion centers bring representatives from local, state, and federal law enforcement agencies to share and analyze criminal intelligence and information about violent extremism.[24] These information-operations centers can monitor social media, news media, and other online information sources; issue advisories; and take other actions to counter false information.

Mitigation

Although the definition of mitigation is "to reduce loss of life and property by lessening the impact of [future] disasters," this definition could be adapted for cognitive defense, to incorporate technological measures that mitigate the impact of false information.[25] Efforts to mitigate the impact of false information must start with social media and technology providers, to identify and flag or weed out disinformation, deepfakes, and bot-generated content.[26] Perhaps the best way to mitigate the effects of disinformation is to introduce legislation requiring social media companies to be more transparent and adapt the algorithms that drive content to preclude the doom spirals that take users deeper into false information.[27]

Response

While serving as the director of intelligence for Joint Task Force North, US Army Colonel Daniel S. Hall recommended creating a new occupational specialty called cyber scouts, who would be trained to "scour the Web and social media platforms for gray propaganda" and false information, and initiate actions to refute that information.[28] Within the nationwide network

of information-operations centers, intelligence on false information could be shared, targeting nonhuman bots for exposure and criminally prosecuting bad actors.

Recovery

Increasingly, foreign disinformation is being targeted toward natural and man-made disasters in the United States, adding to the complexity and consequences of such incidents.[29] As Dr. Mark Landahl points out in his paper, after the train derailment and toxic chemical spill in East Palestine, Ohio, in February 2023, the incident became a target of disinformation and malinformation. Multiple themes emerged, such as claims the government was covering the true extent of the contamination, acid rain was occurring, and journalists were being arrested.[30] In one case, the actual crash of a plane with employees of an environmental consulting firm (responding to an explosion at a metal factory elsewhere in Ohio) was promoted in the cybersphere, raising speculation the crash had some connection with the East Palestine accident.[31] The focus of recovery is to restore and revitalize the fabric of communities affected by a catastrophic incident, so disinformation specialists will need to be deployed on incident-recovery teams to dispel false information directly in the communities affected.[32]

Cognitive Defense and Resilience

As shown in this chapter, resilience is a term used broadly to describe goals for national security, national preparedness, and now the cognitive domain. The definition of resilience provided by Presidential Policy Directive-8—"refers to the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies"—implies wide-ranging meaning applicable across any threat or phase of a disaster.[33] A final recommendation (which this author has previously advocated) is to broaden the definition and application of the resilience core capability beyond just the Mitigation Mission Area where the capability is currently assigned in the NPS, and to add a new capability target that compels leaders in every sector of the homeland security and defense enterprise to reinforce the belief by recognizing the threat, adapting to the challenges, and working together, individuals and communities can withstand and overcome natural and man-made disasters.[34] See figure 3-3.[35]

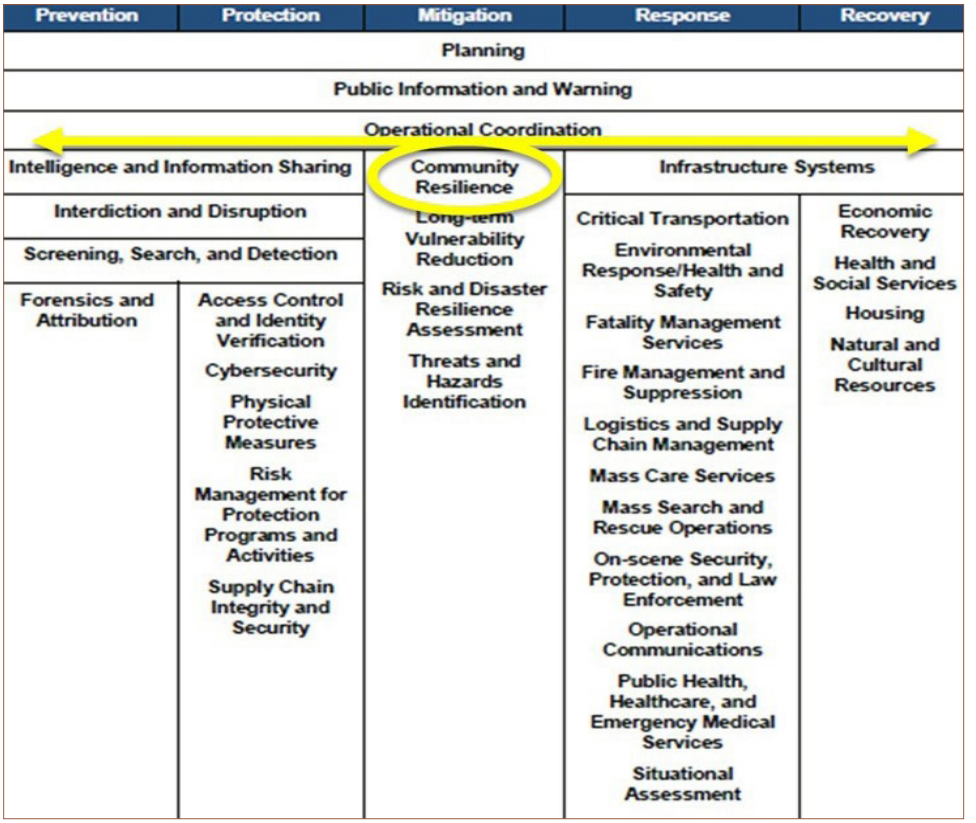


Figure 3-3. Broadening the resilience core capability across the mission areas

Is America Strong?

After many disasters in the United States, communities have risen to the challenges and rallied themselves using slogans that speak to their resilience, such as "Jersey Strong" and "Maui Strong," which is encouraging. But the future of communities' belief in their resilience can be called into question if the speed and volume of cognitive warfare increase and deep divisions within our society become more evident.

The Federal Emergency Management Agency uses a whole-community approach to preparedness before, during, and after disasters by bringing together all community stakeholders, along with their knowledge and resources.[36] With the recognition one's neighbors are often the first to respond after a disaster, part of the intent of the approach is to leverage and strengthen the existing social infrastructure. But only about half of Americans know and trust just some of their neighbors.[37] Robert Putnam, a social researcher, identified Americans are

becoming progressively less civically engaged, and our social connections are thin.[38] The US Surgeon General has even described the increasing rate of social isolation in United States as an epidemic.[39]

Americans' confidence in our major institutions is also at near-historic lows, with an overall trust rating of 26 percent.[40] Although the military is the second most trusted institution at 60 percent, its level of trust has declined by almost 10 points in the last three years. Trust in newspapers and television news is 18 percent and 14 percent, respectively. The *Reuters Institute Digital News Report 2023* indicates that only 32 percent of Americans trust the news, whereas 69 percent of Finns have trusted their news over the last decade.[41] Every one of the three branches of our federal government is at a trust rating of 27 percent or below, with faith in Congress being the lowest at 8 percent.[42] Perhaps most troubling of all is only 28 percent of Americans are satisfied with the way democracy is working in our country—a record low.[43]

Conclusion

With our potential adversaries using cognitive warfare to allow us to destroy our country from the inside out, these data indicate the homeland is not strong.[44] A full-scale war may very well rally the country like a superstorm can galvanize a state. But if foreign competitors can manage the conflict below the level of a full-scale war, they could continue taking advantage of our societal fissures to persuade Americans to become less invested and more distrustful. Our nation invests tremendously in professionals, technologies, and programs that secure and defend our homeland and citizens. That spending could be for nothing if our citizens were led to believe the struggle for the American experiment has already been lost. A whole-of-nation effort is necessary to secure and defend the homeland.

Endnotes

1. Author's note: This chapter includes a reference to another article written by the author but published after the Homeland Defense Symposium.

"The Convergence of National Security and Homeland Security: A Conversation with DHS Secretary Alejandro N. Mayorkas," Center for Strategic and International Studies, December 5, 2022, https://www.csis.org/analysis/convergence-national-security-and-homeland-security-conversation-dhs-secretary-alejandro-n.

2. Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Strategic Studies Institute, US Army War College Press, 2016).

3. US Cybersecurity and Infrastructure Security Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity Advisory AA24-038A (US Cybersecurity and Infrastructure Security Agency, 2024).

4. Heather J. Williams et al., *A Dangerous Web: Mapping Racially and Ethnically Motivated Violent Extremism* (RAND Corporation, 2022); and US Department of Homeland Security (DHS), *Homeland Threat Assessment 2024* (DHS, 2024).

5. "Cognitive Warfare: Strengthening and Defending the Mind," NATO Allied Command Transformation, April 5, 2023, https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

6. Bernard Claverie and François du Cluzel, *The Cognitive Warfare Concept* (NATO Innovation Hub, 2023).

7. Alonso Bernal et al., *Cognitive Warfare: An Attack on Truth and Thought* (NATO, 2020), 3.

8. DHS, *Homeland Threat Assessment 2024*.

9. Sun Tzu, *The Art of War*, trans. S. B. Griffith (Oxford Press, 1963), 77.

10. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton Press, 1984).

11. Clausewitz, *On War*, 77.

12. Clausewitz, *On War*, 30.

13. Clausewitz, *On War*, 50, 54, 68.

14. *The Stanford Encyclopedia of Philosophy*, s.v. "belief," updated November 15, 2023, https://plato.stanford.edu/archives/spr2024/entries/belief/.

15. Daniel S. Hall, "America Must Engage in the Fight for Strategic Cognitive Terrain," *Joint Forces Quarterly* 108, no. 1 (2023): 77.

16. "Strengthening and Defending."

17. Jarrod Brook, "Clausewitz, the Trinity, and the Utility of Hybrid War," *The Strategy Bridge*, September 15, 2020, https://thestrategybridge.org/the-bridge/2020/9/15/clausewitz-the-trinity-and-the-utility-of-hybrid-war.

18. "Presidential Policy Directive / PPD-8: National Preparedness," DHS, updated October 27, 2022, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness; and "National Preparedness Goal," Federal Emergency Management Agency (FEMA), updated March 21, 2023, https://www.fema.gov/emergency-managers/national-preparedness/goal.

19. Headquarters, Department of the Army (HQDA), *The Army in Military Competition*, Chief of Staff Paper #2 (HQDA, 2021).

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

21. Eliza Mackintosh, "Finland Is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy," *CNN*, May 2019, https://www.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

22. Cao et al., "Countering Cognitive Warfare."

23. Sydney J. Freedberg Jr., "Fog of Information War: Army Asks Civilians, Allies for Aid," Breaking Defense, September 25, 2019, https://breakingdefense.com/2019/09/fog-of-information-war-army-asks-civilians-allies-for-aid/; and US Cyberspace Solarium Commission, "Countering Disinformation in the United States" (white paper, US Cyberspace Solarium Commission, December 2021).

24. "Fusion Centers and Intelligence Sharing," Bureau of Justice Assistance, n.d., accessed on April 5, 2024, https://bja.ojp.gov/program/it/national-initiatives/fusion-centers.

25. DHS, *National Preparedness Goal*, 2nd ed. (DHS, September 2015), 10.

26. Bernal et al., *Attack on Truth*.

27. US Cyberspace Solarium Commission, "Countering Disinformation."

28. Hall, "Strategic Cognitive Terrain," 85.

29. DHS, *Homeland Threat Assessment 2024*.

30. Annie Jennemann, "Tackling False Information after the East Palestine, Ohio Train Derailment," PreventionWeb, March 28, 2023, https://www.preventionweb.net/news/tackling-false-information-after-east-palestine-ohio-train-derailment.

31. Andrew Demillo, "5 Die in Small Airplane Crash in Little Rock," Associated Press, February 22, 2023, https://apnews.com/article/little-rock-arkansas-business-plane-crashes-8ee32804f75f8a0054a2e77e9134f2e3.

32. DHS, *National Preparedness Goal*.

33. "Presidential Policy Directive."

34. George Schwartz, "The 'R' word," Domestic Preparedness, April 10, 2024, https://www.domesticpreparedness.com/articles/the-r-word.

35. DHS, *National Preparedness Goal*.

36. FEMA, *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action*, FDOC 104-008-1 (FEMA, December 2011).

37. George Gao, "Americans Divided on How Much They Trust Their Neighbors," Pew Research Center, April 13, 2016, https://www.pewresearch.org/short-reads/2016/04/13/americans-divided-on-how-much-they-trust-their-neighbors/.

38. Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (Touchstone Books, 2001).

39. Office of the US Surgeon General, *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community* (Office of the US Surgeon General, 2023).

40. Lydia Saad, "Historically Low Faith in U.S. Institutions Continues," Gallup, July 6, 2023, https://news.gallup.com/poll/508169/historically-low-faith-institutions-continues.aspx.

41. Nic Newman et al., *Reuters Institute Digital News Report 2023* (Reuters Institute, 2023).

42. Saad, "Faith in U.S. Institutions."

43. Jeffrey M. Jones, "Record Low in U.S. Satisfied with Way Democracy Is Working," Gallup, January 5, 2024, https://news.gallup.com/poll/548120/record-low-satisfied-democracy-working.aspx.

44. Bernal et al., *Attack on Truth*.

Bibliography

Bernal, Alonso, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla. *Cognitive Warfare: An Attack on Truth and Thought*. NATO, 2020.

Brook, Jarrod. "Clausewitz, the Trinity, and the Utility of Hybrid War." *The Strategy Bridge*, September 15, 2020. https://thestrategybridge.org/the-bridge/2020/9/15/clausewitz-the-trinity-and-the-utility-of-hybrid-war.

Bureau of Justice Assistance. "Fusion Centers and Intelligence Sharing." Accessed April 5, 2024. https://bja.ojp.gov/program/it/national-initiatives/fusion-centers.

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

Center for Strategic and International Studies. "The Convergence of National Security and Homeland Security: A Conversation with DHS Secretary Alejandro N. Mayorkas." December 5, 2022. https://www.csis.org/analysis/convergence-national-security-and-homeland-security-conversation-dhs-secretary-alejandro-n.

Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. Princeton University Press, 1984.

Claverie, Bernard and François du Cluzel. *The Cognitive Warfare Concept*. NATO Innovation Hub, 2023.

Demillo, Andrew. "5 Die in Small Airplane Crash in Little Rock." Associated Press, February 22, 2023. https://apnews.com/article/little-rock-arkansas-business-plane-crashes-8ee32804f75f8a0054a2e77e9134f2e3.

Echevarria II, Antulio J. *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*. Strategic Studies Institute, US Army War College Press, 2016.

Federal Emergency Management Agency. *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action*. FDOC 104-008-1. Federal Emergency Management Agency, December 2011.

Freedberg Jr., Sydney J. "Fog of Information War: Army Asks Civilians, Allies for Aid." Breaking Defense, September 25, 2019. https://breakingdefense.com/2019/09/fog-of-information-war-army-asks-civilians-allies-for-aid/.

Gao, George. "Americans Divided on How Much They Trust Their Neighbors." Pew Research Center, April 13, 2016. https://www.pewresearch.org/short-reads/2016/04/13/americans-divided-on-how-much-they-trust-their-neighbors/.

Hall, Daniel S. "America Must Engage in the Fight for Strategic Cognitive Terrain." *Joint Forces Quarterly* 108, no. 1 (2023): 75–86.

Headquarters, Department of the Army. *The Army in Military Competition*. Chief of Staff Paper #2. Headquarters, Department of the Army, 2021.

Jennemann, Annie. "Tackling False Information after the East Palestine, Ohio Train Derailment." PreventionWeb, March 28, 2023. https://www.preventionweb.net/news/tackling-false-information-after-east-palestine-ohio-train-derailment.

Jones, Jeffrey M. "Record Low in U.S. Satisfied with Way Democracy Is Working." Gallup, 2024. https://news.gallup.com/poll/548120/record-low-satisfied-democracy-working.aspx.

Mackintosh, Eliza. "Finland Is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy." *CNN*, May 2019. https://www.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

NATO Allied Command Transformation. "Cognitive Warfare: Strengthening and Defending the Mind." April 5, 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

Newman, Nic, Richard Fletcher, Kirsten Eddy, Craig T. Robertson, and Rasmus Kleis Nielson. *Reuters Institute Digital News Report 2023*. Reuters Institute, 2023.

Office of the US Surgeon General. *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community*. Office of the US Surgeon General, 2023.

Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. Touchstone Books, 2001.

Saad, Lydia. "Historically Low Faith in U.S. Institutions Continues." Gallup, July 6, 2023. https://news.gallup.com/poll/508169/historically-low-faith-institutions-continues.aspx.

Schwartz, George. "The 'R' word." Domestic Preparedness, April 10, 2024. https://www.domesticpreparedness.com/articles/the-r-word.

Tzu, Sun. *The Art of War*. Translated by S. B. Griffith. Oxford Press, 1963.

US Cybersecurity and Infrastructure Security Agency. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

US Cyberspace Solarium Commission. "Countering Disinformation in the United States." White Paper #6. US Cyberspace Solarium Commission, December 2021.

US Department of Homeland Security. *Homeland Threat Assessment 2024*. US Department of Homeland Security, 2024.

US Department of Homeland Security. *National Preparedness Goal*. 2nd ed. Department of Homeland Security, 2015.

US Department of Homeland Security. "Presidential Policy Directive / PPD-8: National Preparedness." Updated October 27, 2022. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

Williams, Heather J., Luke J. Matthews, Pauline Moore, et al. *A Dangerous Web: Mapping Racially and Ethnically Motivated Violent Extremism*. RAND Corporation, 2022.

About the Authors

Mark Landahl, PhD, currently serves as the emergency manager for the city of Rockville, Maryland. Landahl's experience includes serving as the homeland security commander for the Frederick County Sheriff's Office in Maryland, including being responsible for all-hazards preparedness, response, and management of the intelligence function. In addition to professional practice, Landahl teaches emergency management and homeland security courses at Jacksonville State University. He is the coauthor and coeditor of two books and is the author of more than a dozen articles in academic journals and chapters in edited works. Landahl is also an associate editor for the *Journal of Homeland Security and Emergency Management*.

Michael Roi, PhD, is a strategic advisor at the Canadian Joint Operations Command. Roi's experience includes appointments as the head of the policy planning analysis team in the Policy Group of the Canadian Department of National Defence and as the director of strategic operations analysis on the Strategic Joint Staff. His experience also includes serving as a strategic analyst in the Centre for Operational Research and Analysis and as the executive director of the NATO Association of Canada. Roi's academic experience includes teaching history and international relations at the University of Toronto and serving as an adjunct professor at the Royal Military College of Canada in the War Studies Programmes.

George M. Schwartz, EdD, is an associate professor and director of the undergraduate program in Emergency Planning and Management at Immaculata University. Schwartz has a broad professional background that includes active and reserve service in the US Army, human resource management with Fortune 500 companies, and higher education. His military career includes experience commanding troops and directing operations in Europe, Kosovo, and Afghanistan, and managing National Guard emergency-response efforts during several natural disasters in the homeland. Schwartz's experience also includes instructing courses in emergency management and writing and presenting on such subjects as crisis leadership, cybersecurity, and training management. He is also a reviewer for the *Journal of Security, Intelligence, and Resilience Education*.

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers in the global application of Landpower. Concurrently, it is our duty to the Army to also act as a "think factory"for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate on the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The SSI Live Podcast Series provides access to SSI analyses and scholars on issues related to national security and military strategy with an emphasis on geostrategic analysis.

The Center for Strategic Leadership provides strategic education, ideas, doctrine, and capabilities to the Army, the Joint Force, and the nation. The Army, Joint Force, and national partners recognize the Center for Strategic Leadership as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.

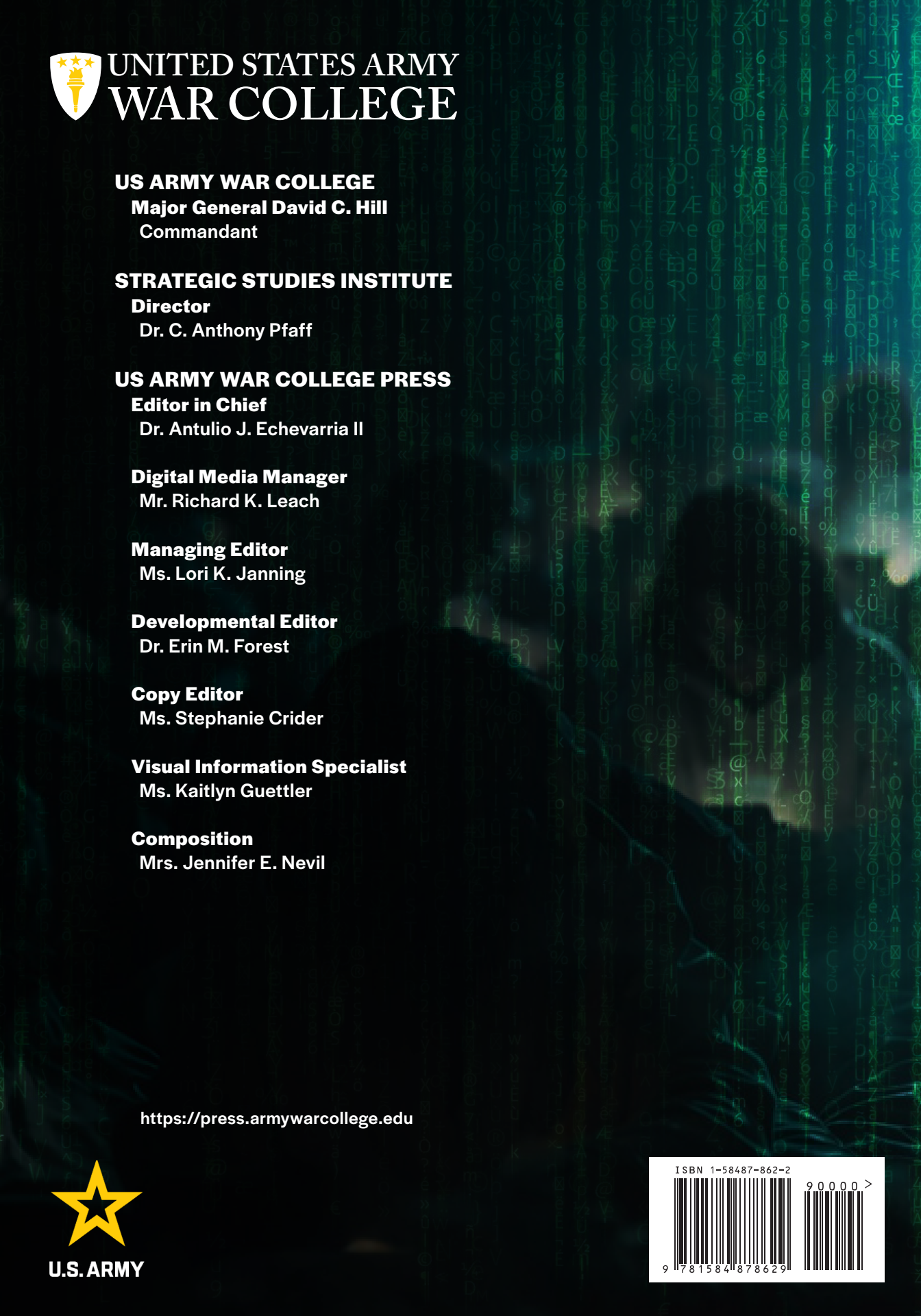
The School of Strategic Landpower provides support to the US Army War College purpose, mission, vision, and the academic teaching departments through the initiation, coordination, and management of academic-related policy, plans, programs, and procedures, with emphasis on curriculum development, execution, and evaluation; planning and execution of independent and/or interdepartmental academic programs; student and faculty development; and performance of academic-related functions as may be directed by the commandant.

The US Army Heritage and Education Center engages, inspires, and informs the Army, the American people, and global partners with a unique and enduring source of knowledge and thought.

The Army Strategic Education Program executes general officer professional military education for the entire population of Army general officers across the total force and provides assessments to keep senior leaders informed and to support programmatic change through evidence-based decision making.

The US Army War College Press supports the US Army War College by publishing monographs and a quarterly academic journal, *Parameters*, focused on geostrategic issues, national security, and Landpower. Press materials are distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities. The US Army War College Press serves as a bridge to the wider strategic community.

The US Army War College Press produces two podcast series. Decisive Point, the podcast companion series to the US Army War College Press, features authors discussing the research presented in their articles and publications. Visit the website at: https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Decisive-Point-Podcast/. Conversations on Strategy, a Decisive Point podcast subseries, features distinguished authors and contributors who explore timely issues in national security affairs. Visit the website at: https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Conversations-on-Strategy-Podcast/.



UNITED STATES ARMY
WAR COLLEGE

https://press.armywarcollege.edu

U.S. ARMY

ISBN 1-58487-862-2
9 781584 878629
90000