Hudson Institute

MAY 2024

Cognitive Competition, Conflict, and War: An Ontological Approach

ROBERT "JAKE" BEBBER, PHD
ANDREW W. MARSHALL SCHOLAR, HUDSON INSTITUTE

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, energy, technology, culture, and law.

Hudson seeks to guide policymakers and global leaders in government and business through a robust program of publications, conferences, policy briefings, and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue, NW
Fourth Floor
Washington, DC 20004

+1.202.974.2400
info@hudson.org
www.hudson.org

Cover: (Getty Images)

Hudson Institute

MAY 2024

Cognitive Competition, Conflict, and War: An Ontological Approach

ROBERT "JAKE" BEBBER, PHD
ANDREW W. MARSHALL SCHOLAR, HUDSON INSTITUTE

ABOUT THE AUTHOR

Robert "Jake" Bebber is an officer in the United States Navy. He has served at various locations throughout his career, including Fort Meade, US 7th Fleet, Carrier Strike Group 12, Information Warfare Training Command-Corry Station, and US Special Operations Command. He holds a PhD in public policy from the University of Central Florida. His writings have appeared in *Proceedings, Orbis, Journal of Information Warfare, Journal of Political Risk, Comparative Strategy,* and elsewhere. He is supported by his wife, Dana, and their two boys, Vincent and Zachary. Jake welcomes your comments at jbebber@gmail.com.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank the following individuals who kindly reviewed this draft and previous versions, providing critical feedback and recommendations. Their contributions have made this report better. Any remaining errors and deficiencies are my own.

Capt. (Ret.) Ric Arthur
Dr. Bruce Berkowitz
Mr. Jeff Becker
Ms. Cyan Bannister
Mr. Christopher Brown
Mr. Shuvo Chatt
Dr. Jacqueline Deal
Dr. Michael Fischerkeller
Dr. Melissa Flagg
Mr. Matthew Frendewey
Mr. Robert Giesler
Mr. Paul Giarra
Dr. Emily Goldman
Dr. James Giordano
Dr. Richard Harknett
Ms. Jane Horton
Lt. Col. Brian Kerg
Ms. Elsa Kania
Dr. Darren Lawrence
Mr. Sorin Lungu
Dr. Dominique J. Monlezun
Dr. Claire M. Modica
Mr. Constantine Nicolaidis
Mr. James Proud
Dr. Samantha Ravich
Mr. Jason Reed
Dr. Maureen Rhemann
Capt. (Ret.) Benjamin Riley
Mr. Dale Rielage
Dr. Adam Russell
Dr. Peter Singer
Dr. Adam L. Silver
Mr. Arthur Tellis
Dr. Michael Warner
Dr. Treston Wheat

I am grateful to Mr. Constantine Nicolaidis for his assistance with the illustrations.

This report was supported by the Andrew W. Marshall Foundation and the Hudson Institute. I would especially like to acknowledge the additional feedback and editorial recommendations from Mr. Jaymie Durnan and Ms. Stephanie Papa from the Marshall Foundation, and Dr. Bryan Clark and Dr. Dan Patt from the Hudson Institute. Their support and resources made this project possible.

EXECUTIVE SUMMARY

The character of war has evolved from the precision strike and stealth regime developed in the late Cold War–era to operations and technologies that target an opponent's decision-making. This shift has taken many forms, such as gray zone operations, hybrid warfare, little green men, and salami-slicing operations and tactics. Cognitive warfare represents the culmination of this evolution in how countries conduct military operations and calls into question whether traditional kinetic operations alone are necessary to achieve an aggressor's objectives.

Cognitive warfare is highly disruptive, threatening democratic institutions and sovereignty and likely changing the character of war and perhaps analysts' understanding of conflict. The convergence of advances in brain sciences, data and computational technologies, and algorithm-based attention models has fundamentally altered the global strategic environment, expanding the attack surface that foreign adversaries can exploit using cognitive manipulation. Thus far, policymakers in the United States have been slow to diagnose and react to cognitive warfare not only because of its novelty but also perhaps because the American public has remained under a persistent state of cognitive manipulation, which has debilitated the people.

This report builds on Andrew F. Krepinevich's analysis in *The Origins of Victory*, which emphasizes that the world is facing a shift in military affairs.[1] The United States' precision-strike advantage has eroded, and disruptive technologies like artificial intelligence, quantum computing, and synthetic biology are reshaping warfare dynamics. China and Russia are contesting and, in some cases, achieving overmatch against the US military, with ambitions of reshaping the global order.

The emergence of cognitive warfare—which manipulates cognition to destabilize sociocultural, economic, political, and military systems—poses a unique threat to America and its allies. This type of warfare differs from information warfare[2] in that it aims to influence *how*, not *what*, people think, feel, and act, altering the cognitive space from individual to population levels.

Key components of cognitive warfare include its tactical and strategic use, manipulation of the way people think, reliance on brain science and data, and ability to employ multiple engagement modes. The use of algorithm-based computational propaganda and the ability to create self-sustaining feedback and amplification loops are significant features.

The US Department of Defense (DoD) as well as the North Atlantic Treaty Organization (NATO) and other allies have acknowledged the changing character of warfare and the implications of failing to meet the associated challenges. Operations will become fractured, disjointed, and ultimately ineffective as enemies disrupt or destroy linkages and network connections. Perhaps most insidiously, the military may find itself *irrelevant to adversary operations* as cognitive warfare capabilities emerge and mature to the point where adversaries can coerce societies through so-called information confrontation. The US and its allies are likely to find themselves outflanked in the battle space, either ineffective or unable to respond because adversaries can reach into entire domestic populations. Despite this danger, US and allied military forces and national security policymakers have not yet organized their institutions and infrastructure to detect, track, and combat cognitive warfare campaigns that adversaries are waging against the American public. Moreover, Washington and its partners have not developed the operational concepts and requirements necessary to employ their own cognitive warfare capabilities in support of their security needs.[3]

To understand the effects of cognitive warfare and to operationalize defensive measures in support of national security decision-making, one needs to construct a mental framework for how it appears and operates on human beings. The first step in building this framework is to construct an ontology—a formal system for organizing knowledge. The National Academies of Science, Engineering, and Medicine (NASEM) define an ontology as a formal knowledge organization system, which serves as a shared conceptualization and framework for understanding complex relationships. In this context, the NASEM's 2022 report *Ontologies in the Behavioral Sciences* serves as a crucial reference.[4] It highlights the significance of ontologies in the behavioral sciences, a relevance that extends to the environments of competition and conflict.

The use case, a concept that originated in software engineering, can help readers design the ontology. In this report, use cases are narrative scenarios that illustrate how individuals interact with a system to achieve objectives. Engineers structure use cases around five parameters: actors, context, resource, expected outcome, and stakeholders. In the context of competition and conflict in the cognitive space, this model identifies and categorizes ontological elements.

The following proposed tool dimensions provide a comprehensive framework for understanding the multifaceted nature of cognitive warfare:

1. **Tools exploiting cognitive biases and perception:** These threats manipulate individuals' cognitive biases and perceptual vulnerabilities to shape their opinions and behavior.
2. **Tools involving neuroscience and biology:** Adversaries leverage advances in neuroscience and biology to influence and control the cognitive processes of individuals.
3. **Tools exploiting social psychology and group dynamics:** Adversaries harness social psychology and group dynamics to manipulate group behavior, create polarization, or influence collective decision-making.
4. **Tools employing techno-social applications:** Adversaries use information technology to disseminate narratives, engage in social engineering, and conduct information operations.
5. **Tools related to information technology:** Information technology provides tools for cyberattacks, disinformation campaigns, and the disruption of critical infrastructure.

These tool dimensions serve as a foundation for constructing an ontology that systematically categorizes and organizes the diverse aspects of cognitive warfare. The ontology encompasses elements such as classes, attributes, properties, and hierarchies to provide a structured understanding of the cognitive domain. It acknowledges the dual-use nature of these dimensions, in which they represent both threats and opportunities. It also highlights the overlap between technological threats and cognitive threats.

The proposed cognitive warfare ontology offers a tool for understanding and countering cognitive threats. By categorizing and interconnecting the diverse aspects of cognitive warfare, it aids in the identification of vulnerabilities, the development of countermeasures, and the assessment of opportunities. It empowers national security decision-makers with actionable strategies and operational concepts tailored to the cognitive space. As cognitive warfare evolves, continuous refinement, integration into existing security protocols, and collaboration among experts from various fields should enhance the ontology's capabilities. The ethical and legal dimensions of cognitive warfare, privacy concerns, and international cooperation also require attention.

The cognitive warfare ontology, shaped by the forces of neuroscience, technology, and influence, is a crucial tool in navigating this complex and evolving topic. Through research, adaptability, and a forward-thinking approach, the United States can secure its cognitive spaces in an era defined by cognitive warfare.

INTRODUCTION

Andrew F. Krepinevich argued recently in *The Origins of Victory* that the world finds itself today in the midst of a new period of disruption in military affairs. The precision-strike regime that the United States developed in the late Cold War has matured to the point that the US no longer enjoys an overwhelming advantage over peer competitors. Technologies that are disruptive not only in degree but also in kind—such as artificial intelligence, additive manufacturing, quantum computing, and synthetic biology—are reshaping the character of warfare. Communist China and Russia have introduced conventional capabilities at scale to contest, and in some cases overmatch, US conventional forces in most domains. These adversaries are now reshaping the global order to their advantage and, in the case of Communist China, intend to achieve global hegemony. While national security experts largely agree that the Chinese Communist Party (CCP) and Russia threaten American security, there remains no consensus on the direction the US should take to address these threats. Neither political nor military leadership has united around operational challenges on which to focus the military's efforts toward disruptive innovation.[5]

There is nothing new about using information-based strategies to achieve strategic aims. While strategists often hold up the ancient aphorism "Divide and conquer" as a model, classical theorists such as Sun Tzu, Aristotle, Niccolò Machiavelli, and even William Shakespeare suggest the best way to divide enemies—either internally or in alliances—is to

Photo: A woman wears a brain monitoring machine by the Chinese company Yiruide Group at the 2024 World Health Expo in Wuhan, China, on April 7, 2024. (Photo by STR/AFP via Getty Images) break their mutual trust. As Michael Warner and John Childress note:

> Clever sovereigns and commanders thus seek to suborn, confuse, deceive, or mislead their adversary's subjects, supporters, and allies to drive down the willingness of their foes to collaborate. They do so by flooding their foes with too much information to process, confirming foes' biases while hiding key elements and clues to their real intentions, and especially by making adversaries afraid of each other. In short, effective rulers and generals do what they can to break down trust among their opponents.[6]

Perhaps the most disruptive development in global security is the emergence of new forms of warfare beyond the traditional kinetic, conventional space and the nuclear space. This should not be surprising because nuclear and non-nuclear powers will naturally seek ways to achieve their strategic aims while reducing the risk of open conflict and potential nuclear escalation. The approaches that strategists previously referred to as hybrid warfare, asymmetric warfare, and gray-zone warfare, among others, did not have the system-destruction potential that emerging strategies may cause today or in the near future. Those older strategies are still just as concerned about occupying physical space as they are about influencing the decision space. In contrast, cognitive warfare need not rely on the occupation of physical space (see figure 1). This is due to the rapid advancement in the understanding of the human brain, the ability to operationalize that understanding through science and technology, and the economic factors driving the rapid adoption and use of incentive behavior models. The convergence of these forces through leveling technologies makes what humanity once thought impossible or improbable, doable: the employment of non-kinetic, difficult-to-attribute warfare capabilities and campaigns that can assess, access, and affect the cognitive space in novel ways, from the individual to groups and populations, at the tactical to strategic levels. The aspirations of what analysts now call cognitive warfare are on the verge of realization.

This report defines *cognitive warfare* as the following:

> The employment of science and technology that alters cognition within individuals, groups, and populations, thereby leading to changes in understanding, emotion, and behavior. Its aim is to incur disruptive influence in either direct or indirect propagative ways by altering the sensations, perceptions, beliefs, thought patterns, emotions, and resulting behaviors of individuals and collectives so as to destabilize and directionally manipulate the sociocultural, ecological, economic, political, and military status quo and thus to enable intentional leverage and power. Key features include the applications of advanced understanding and methods of the brain sciences, the reliance on data and computational sciences and technologies, the use of the electromagnetic spectrum, and social media driven at varying speeds and scales to target key agents, actors, groups, and populations who may in turn exert behaviors that amplify disruptive effects in particular scales and directions.

Key components of cognitive warfare are as follows:

- States employ it at the tactical and strategic levels to attack competitor or adversary individuals, groups, or systems.
- Combatants use it to influence and direct the way people think, not necessarily what they think. It creates a high level of entropy by attacking trust in systems and institutions.
- It leverages advanced understanding and methods of the brain sciences (bugs, drugs, toxins data,[7] devices) to affect individual and group decision-making.
- It can (either singularly or concomitantly) employ multiple modes of engagement, from influence to manipulation to control of individuals, groups, and populations.
- It adopts and adapts many aspects of behavioral and attention-based economics, using the new narratives, semi-

otics, and constructs to influence and control the underlying network dynamics of various aspects and scales of human ecologies and systems (supply chains, hardware, software).

- It leverages algorithm-based capabilities using computational propaganda.
- Cognitive warfare capabilities can create their own self-sustaining feedback and amplification loops.

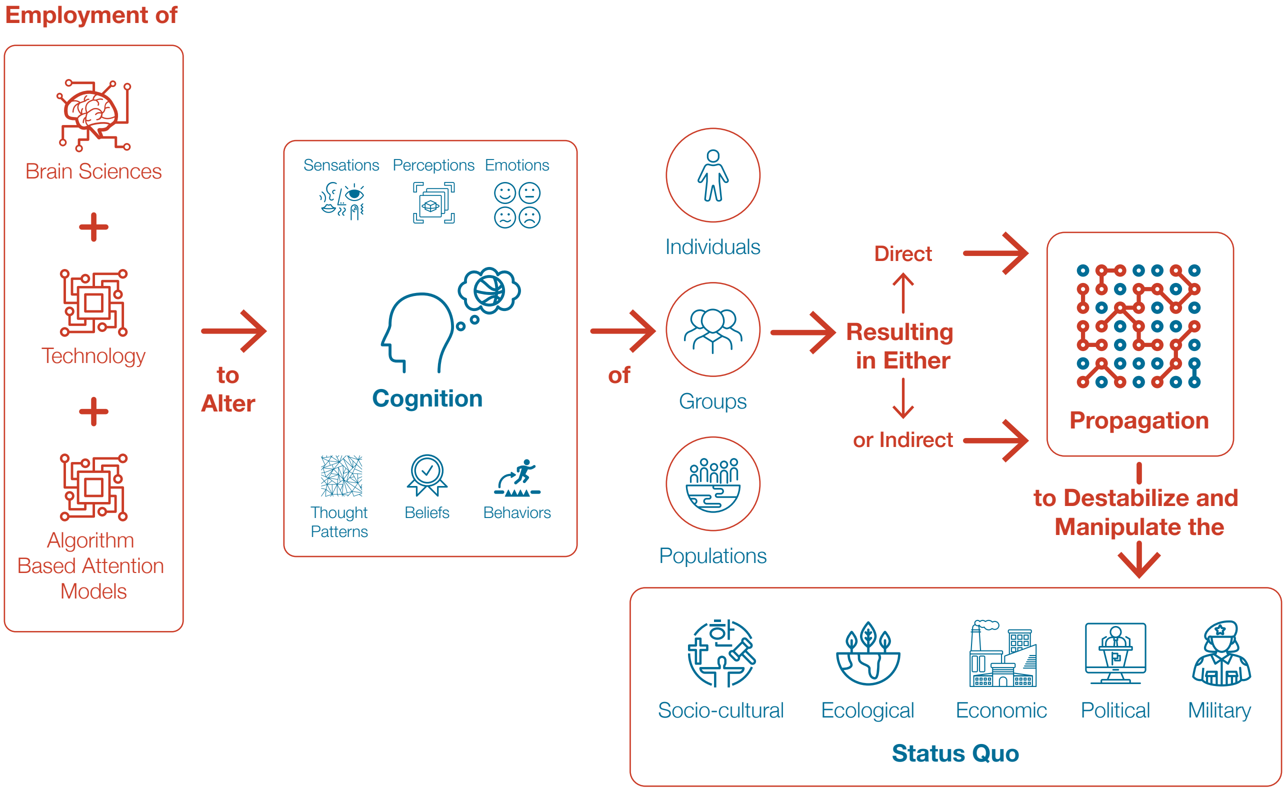
It is essential to note that cognitive warfare extends beyond traditional information operations (i.e., influence, propaganda, and manipulation of public opinion). These soft power aspects of information operations can be an integral component of cognitive warfare,[8] which has caught the attention of US allies. For example, NATO has established the Center for Excellence in Strategic Communication, which conducts research to support counter-disinformation campaigns and addresses the implications for alliance security and the complex challenges that cognitive warfare imposes. Studies that NATO has published thus far underscore the fact that cognitive warfare is an integral part of society with broader social implications, alluding to the need to protect democratic systems and institutions. They highlight not only the role of narratives in manipulating perception and opinion but also the growing use of advanced neuroscience and technology to manipulate and control populations, distinguishing cognitive warfare from traditional information operations.[9]

The Department of Defense Strategic Multilayer Assessment has taken a multidimensional approach to comprehending the complexities of information-age conflict, hoping to provide policymakers with strategies to counter adversary cognitive warfare campaigns. Their studies and presentations have highlighted ethical considerations associated with cognitive warfare, noting that the potential for exploiting technology in conflict requires ethical boundaries, especially in the emerging fields of neuroscience and synthetic biology. Military institutions are also keenly interested in understanding human physiology in warfare, including the monitoring and manipulation of physiology to evaluate and enhance combat effectiveness. The interplay between different cultural factors and their roles in understanding the so-called will to fight, as well as the behavioral and psychological aspects of different actors in war, is receiving considerable attention. Finally, modeling and simulation can offer insights that assist with anticipating future challenges and identifying potential strategic latencies and opportunities for strategic advantage.[10]

Research institutions, universities, and think tanks have invested considerable resources in attempting to identify, analyze, define, combat, and even conduct cognitive warfare. RAND has produced research on a wide range of topics related to information warfare and strategic communications.[11] Universities such as Oxford and Georgetown have established centers and programs focused on disinformation, misinformation, and the role that brain science and information technology plays in shaping human behavior. The Defense Advanced Research Projects Agency (DARPA) has sponsored several programs focused on understanding and countering cognitive warfare, including narrative networks, programs to model social media network influence and manipulation, and the development of tools to rapidly assess human cognitive states in response to stimuli and the global modeling of policy decisions.

The DoD as well as NATO and other allies have acknowledged the changing character of warfare and the implications of failing to meet the associated challenges. Operations will become fractured, disjointed, and ultimately ineffective as enemies disrupt or destroy linkages and network connections. Perhaps most insidiously, the military may find itself *irrelevant to adversary operations* as cognitive warfare capabilities emerge and mature to the point where adversaries can coerce societies through information confrontation. The US and its allies are likely to find themselves outflanked in the battle space, either ineffective or unable to respond because adversaries can reach into entire domestic populations. Despite this danger, US and allied military forces and national security policymakers have not yet organized their institutions and in-

Figure 1. Notional Sketch of Cognitive Warfare Campaigns



Source: Author.

frastructure to detect, track, and combat the cognitive warfare campaigns that adversaries are waging against the American public. Moreover, Washington and its partners have not developed the operational concepts and requirements necessary to employ their own cognitive warfare capabilities in support of their security needs.[12]

This report will highlight what makes cognitive warfare highly disruptive, threatening the core legitimacy of democratic institutions and political sovereignty. It will posit the need for a framework to operationalize the cognitive space, but before policymakers can accomplish operationalization, an ontology will be necessary. While a comprehensive ontology is beyond the scope of this report, the following section will propose some top-level classes or concepts, attempting to define some attributes and properties. From this rough sketch, we might identify potential use cases and threat elements that will help formulate a definition of *cognitive war*. Finally, the report will propose ways in which the US and its allies should operationalize the space and suggest future research questions.

Photo: A man holds a smartphone iPhone screen showing various social media apps on March 13, 2024, in Bath, England. (Photo by Anna Barclay/Getty Images)

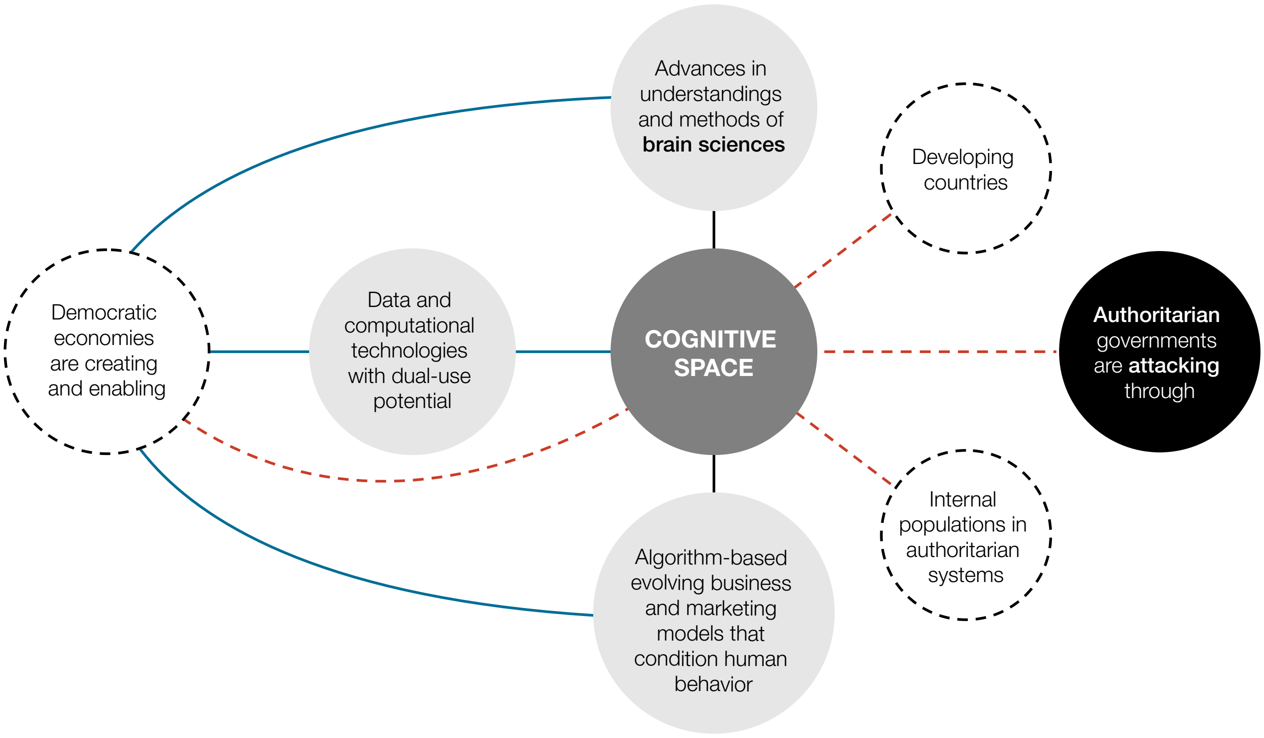
THREE FORCES SHAPING GLOBAL POWER COMPETITION

Global power competition in the twenty-first century is being shaped in part by the convergence of three forces: (1) advances in understandings and methods of brain sciences, (2) growth in the use of and reliance on data and computational technologies with dual-use potential, and (3) algorithm-based evolving business and marketing models that condition human behavior (see figure 2). Chinese policies and investment decisions are creating and exporting a techno-authoritarian information control regime. At the same time, global technology companies are deploying anticipatory decision-based modeling systems designed to create the conditions in consumer environments that shift from predicting consumer desires and having products available to *conditioning consumers to desire the product*. This has changed the global strategic environment and threatens the efficacy of American assumptions about strategic competition and cooperation. Indeed, it expands the attack surface of the American population to cognitive manipulation and control by foreign adversaries.

Emerging Trends in Neuroscience

> **“Speaking of a future at most only decades away, an experimenter in intelligence control asserted, ‘I foresee a time when we shall have the means and therefore, inevitably, the temptation to manipulate**

Figure 2. Forces Shaping the Cognitive Space


Advances in understandings and methods of **brain sciences**
Developing countries
Democratic economies are creating and enabling
Data and computational technologies with dual-use potential
COGNITIVE SPACE
Authoritarian governments are **attacking** through
Internal populations in authoritarian systems
Algorithm-based evolving business and marketing models that condition human behavior

Source: Author.

> **the behavior and intellectual functioning of all the people through environmental and biochemical manipulation of the brain.'"**
>
> *—Zbigniew Brzezinski, Between Two Ages: America's Role in the Technotronic Era (1970)*[13]

The study of the human brain and its applications to warfare and security are not new in human history. Understanding the psychological state of one's own forces as well as the enemy's is necessary to gain strategic advantage. Commanders and political leaders have had to take care to keep their armies and their populations motivated during war and address their anxieties. In the cacophony of a battle, where forces can be spread across miles of space, timely decision-making and effective command and control often dictate the outcome. It has remained a long-held desire to win without fighting by using strategies of influence, intimidation, and deception to encourage or force the capitulation of adversaries. Ancient commanders from Alexander to Genghis Khan well understood the utility of force and employed diplomacy as well as what one would now call psychological and influence operations to achieve their strategic aims.

Today, national security institutions are leveraging advances in neuroscience and associated technologies in ways that were once considered science fiction. Jonathan Moreno's 2006 book *Mind Wars: Brain Research and National Defense* provides a historical overview of US government–led research efforts in neuroscience and technology going back to the Cold War. Technologies he discusses in his work include neuroimaging; brain-machine interfaces; "augmented cognition," or attempts to improve human cognition; and the use of pharmaceuticals to improve cognitive and physical performance. Importantly, he identifies the ethical, legal, and regulatory uses of neuroscience and technology and their implications for national security.[14]

Since 2006, improvements in the understanding of brain functions and their applications to national security have only accelerated. State actors, especially techno-authoritarian powers, are devoting considerable resources to the development of neuroweapons and synthetic biology with the desired effects of manipulating cognitive and emotional states. They can use these technologies as soft weapons to create economic leverage, intelligence capabilities, and advanced psychological influence operations, such as narrative networks. More concerning is the way neuroscience is informing the development of hard weapons that can have physical effects using chemicals, biologicals, toxins, and devices. When coupled with the growing availability of biodata, including genetic and biological information, the dual uses of synthetic biology and neuroscience are apparent. Neuromodulating bioagents like opioids (such as fentanyl), enzymes, immune and inflammatory modulators, CRISPR-gene-edited agents to create "precision pathologies," and even nanoneurotechnologies that can be aerosolizable may not be very far in the future.[15] Governments are increasing research investments in brain and biological functions that can apply to military, intelligence, and strategic objectives.[16] As these advances continue, policymakers need to navigate complex ethical and security dilemmas concerning privacy, consent, threats, and the potential misuse of neurotechnology and synthetic biology in the context of national security.[17]

Potentially, neuroscience and technology can study, define, predict, and influence human activities on the individual, group, and population levels. These actions can have systemic effects across local, regional, and global scales and can transform the conduct and understanding of national security and defense. Brain assessment techniques such as neuroimaging, neurophysiological recording, neurogenomics and genetics, neuroproteomics, and neuro-cyber informatics have made possible more interventional technologies, such as cyber-lined neurocognitive manipulation, directed energy devices, novel pharmaceuticals, and organic neurotoxins. Scientists are weaponizing these technologies in the form of chemicals, biologicals, devices, and neuroweapons. Potentialities include the use of pharmaceuticals and organic neurotoxins against specific, high-interest targets; neuro-microbiologic agents that have psychiatric effects on groups and populations; and even neurovascular hemorrhagic agents (targeting individuals or creating "stroke epidemics"). It may soon be possible to use high-output sensory stimulators and even neural network disruptions ("confusion generators" and "time warpers").[18]

Strategic competitors have invested considerable resources into the research, development, and fielding of neuroscience and biotechnology. China has announced initiatives to position itself as the leading power in brain science and is openly exploring the application of brain sciences to hard and soft power. Military writers and researchers in China argue that future battlefield success will depend on "biological dominance," "mental/cognitive dominance," and "intelligence dominance" and are applying their own insights from neuroscience to exploit vulnerabilities in human cognition, including the development of "brain control weaponry."[19] China's People's Liberation Army (PLA)—the military wing of the CCP—has adopted a holistic concept of influence operations, emphasizing the military's comprehensive approach to shaping narratives and perceptions.[20] Their information warfare capabilities intertwine with their cognitive warfare strategies. China has developed sophisticated techniques for cyber operations, which it uses not only for espionage but also for psychological warfare, affecting its adversaries' perceptions and cognitive processes.[21] These tactics align with China's strategic approach, in which it aims to win without fighting by shaping global narratives and perceptions to further its interests.[22]

China's advanced technological capabilities, including AI and surveillance, are also pivotal in its cognitive warfare efforts. It uses these technologies to monitor and control information flows, thereby influencing the cognitive environment both domestically and globally.[23] Its control over widely used social media applications, such as TikTok and WeChat, as well as the underlying telecommunications infrastructure creates cognitive manipulation opportunities through algorithm-driven content recommendations and the sharing of personal data with Chinese security and intelligence. It also serves as a propagation tool for misinformation and disinformation campaigns and has a profound effect on American mental health.[24] In sum, China's strategic employment of neuroscience and cognitive warfare is a multifaceted approach that encompasses information operations, cyber capabilities, and biotechnology, all aimed at gaining an advantage in shaping perceptions, controlling narratives, and advancing its national security objectives.

Russia has been employing cognitive warfare tools as a geopolitical strategy for decades and has recently emphasized the blend of its concept of active measures with cyber operations to shape narratives, influence perceptions, and undermine the stability of democratic states. These tactics include the dissemination of false or misleading information, propaganda, and the use of cyber operations to infiltrate and disrupt digital infrastructures.[25] Russia's largely successful employment of cognitive warfare and information-related capabilities eliminates the binary boundary of peace and war, creating a conflict continuum across the cognitive space that is both multifaceted and targeted to specific populations, whether NATO members, the American voter, or its own population.[26]

Data, Sensors, and Emerging Computational Technologies

> **"Science and technology has become the main battleground of great power rivalry."**
>
> *—Xi Jinping*[27]

The race to acquire advanced technologies in data storage, ubiquitous sensors, autonomous systems, human-machine teaming, and powerful computational technologies—all of which have cognitive warfare potential—will shape the emerging world order. The barriers to entry for these information-related technologies have dropped substantially, creating a global diffusion and proliferation regime in which any actor can access potentially disruptive technologies.

Data has become a strategic asset to harvest and exploit for oneself while denying it to an adversary in conflict.[28] Governments, corporations, businesses, civic organizations, criminal organizations, nonprofits, violent extremists, and individuals are collecting and analyzing vast amounts of data to gain insights for their strategic purposes. Those who can harvest and process data efficiently and effectively realize competitive advantages. Advanced data storage and processing are enabling exponential growth in machine learning that is steering sophisticated artificial intelligence applications. This growth is driving the development of human-machine teaming systems that seek to improve decision-making and operational effectiveness.[29]

AI and machine learning algorithms can automate the generation of targeted content, deepfakes, and personalized disinformation, making it easier to spread false information and manipulate public opinion. The ubiquity of sensors enabling the collection of real-time data connected to the Internet of Things and satellites can supply a holistic view of populations. Regimes can exploit this technology to gain insights into public sentiments, movements, vulnerabilities, or threats against them.[30]

Powered by AI and machine learning, autonomous systems can execute cyberspace operations, including malware deployment, without human intervention, thereby obfuscating attribution while enabling covert offensive operations.[31] Collectively, these technologies contribute to cognitive warfare by facilitating the creation and dissemination of disinformation, propaganda, and targeted influence campaigns as well as sophisticated and effective manipulation of the cognitive environment.

Technical advancement in quantum computing has great potential cognitive warfare effects because it is revolutionizing the fields of information processing and encryption. With the power of quantum computation, adversaries may be able to break current encryption methods, allowing access to sensitive information. Quantum computing can enable more efficient and sophisticated data analysis, providing the means to create highly convincing disinformation campaigns and perhaps manipulate the cognitive environment on an unprecedented scale. While still in its nascent stage, it has powerful cognitive implications.[32]

Algorithm-Based Business, Marketing, and Financial Models

> **"You get a show or a movie you're really dying to watch, and you end up staying up late at night, so we actually compete with sleep."**
>
> *—Reed Hastings, CEO of Netflix*[33]

The American public remains under a persistent state of cognitive manipulation. As the information-based economy has grown, so too have economic interests that leverage advances in neuroscience and dual-use technologies to shape consumer preferences and behavior. And as the above quote from Reed Hastings suggests, businesses have a growing financial interest even in altering biological needs such as sleep patterns, contributing to cognitive performance problems in order to maximize profitability.

Algorithm-driven business marketing models leverage insights from neuroscience to shape and potentially control human behavior. Neuroscience research is informing these industries by providing valuable insights into the human brain's responses and preferences, allowing businesses to optimize their strategies for maximum impact. Companies are using techniques like neuromarketing that combine psychology and neuroscience to design marketing campaigns that appeal to consumers on a subconscious level. These campaigns tap into cognitive processes and emotional responses, ultimately influencing consumer choices and preferences.[34]

Neuroscience findings are particularly valuable in the context of the "attention economy," in which companies compete for consumers' limited attention. By understanding the brain's mechanisms of attention and cognition, businesses can design more captivating and persuasive content. Furthermore, the digital economy relies heavily on user data and the optimization of digital platforms. Here, neuroscience contributes to enhancing user experiences and fine-tuning algorithms to ensure consumers remain engaged and responsive.[35]

Neuroscience is also reshaping financial services. This sector leverages data analytics and user-centric design to create more intuitive and persuasive financial products and interfaces. This approach aims to foster trust and loyalty, ultimately affecting consumer decisions related to financial technology.[36]

Convergence: Are Cognitive Campaigns Achieving System Destruction?

Advances in the neurosciences—and in the application of information technology at speed and scale toward these new understandings to shape and perhaps control human behavior at the individual, group, and population levels—have potential system-disruptive and *-destructive* effects that are likely overwhelming policymakers and national security decision-making processes. America's adversaries in Communist China and Russia are certainly employing cognitive campaigns against the

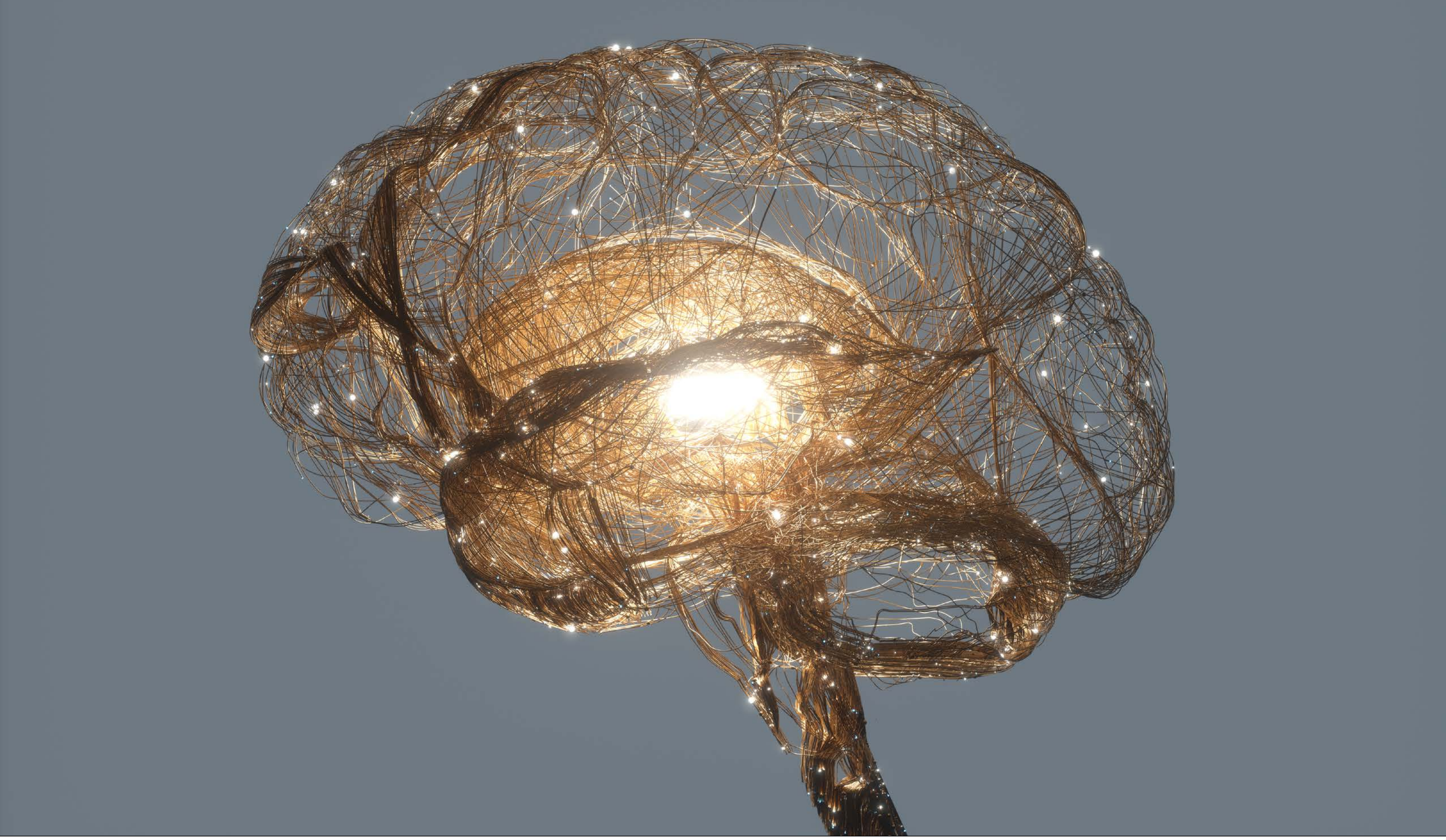
American public, but global technology companies, corporations, political advocacy institutions, and nonstate actors are also leveraging neuroscience and technology in support of their business interests, marketing strategies, public-opinion shaping, and even criminal enterprises. The American polity itself may be exhibiting the effects of these campaigns with disastrous results for the social systems necessary for a functioning democracy.

Studies and reporting suggest that algorithm-driven applications, social media, and technology are shaping public behavior with significant public health impacts. For example, research has highlighted that as social media has become integral to modern life, especially among young adults, there has been a dramatic increase in social media addiction, anxiety, and depression.[37] Studies highlight the effects of social media use on self-esteem and body image as well as the potential for cyberbullying and harassment.[38] Research further suggests that young adults are more hesitant to approve of the use of force to protect national security interests and may not share attitudes that value America's place in the world.[39] This hesitation presents the worrisome prospect that in the event of a national emergency, the populations that the nation relies on for political survival may not be inclined to defend it—or may participate in achieving US adversaries' strategic objectives. The fact that CCP-controlled social media platforms such as TikTok and WeChat continue to operate within the American information ecosystem keeps open their attack vector into the American public and especially young adults, allowing the CCP to mold, shape, and potentially control American public behaviors in support of its systems-destruction strategies.[40]

Meanwhile, attention-based economic models driven by social media and online entertainment platforms rely on holding consumer engagement. This often involves the use of algorithms that prioritize sensational and emotionally charged content, which can lead to addictive behaviors and emotional distress. These platforms are designed to capture and maintain users' attention, often at the expense of their well-being.[41]

Since 2012, studies have suggested that social media use also amplifies political polarization. Neurotechnology is informing the design of algorithms and technology to appeal to individual cognitive biases and emotional responses. People naturally self-select into social media platforms that reinforce preexisting belief systems, creating echo chambers and inhibiting critical thinking. This polarization is contributing to social unrest, political violence, and dysfunctional governance. It has also contributed to widespread belief in conspiracy theories and the erosion of trust in information sources outside one's self-selected information ecosystem. Online social media participation can thus reinforce false beliefs, shaping public behavior.[42]

Given the difficulty of unwinding the neurological and psychological pathways of behavior, analysts may have to accept that they know *exposure* to cognitive campaigns can influence people's behavior and that there is likely a neurological component. Applications of neurotechnology are only amplifying these pathways and system effects. While analysts do not yet fully understand those pathways, they should pay attention to the social and behavioral aspects that would allow them to solve the parts of the problem they can observe and, through observation, develop their own effective counter-cognitive campaigns as well.



OPERATIONALIZING THE COGNITIVE SPACE: THE NEED FOR AN ONTOLOGY

In the context of cognitive warfare and information operations, operationalizing the cognitive space refers to the systematic and structured approach required to understand, influence, and manipulate the cognitive aspects of human behavior, perception, and decision-making. This includes understanding how individuals process information, form beliefs, and make decisions, which are crucial elements in the realm of cognitive warfare. To achieve this goal, an ontology is essential. This report will first propose examples, or use cases, that define how an actor or actors might employ cognitive warfare operations and whom these operations might affect, the tools and attributes associated with such operations, and finally a proposed framework for the ontology. Importantly, these tool dimensions represent both threats and opportunities for American and allied planners.

The NASEM define an *ontology* as "a formal system for organizing knowledge." It is an explicit, formal specification of a shared conceptualization—a systematic set of shared terms and an explication of their interrelationships. Their 2022 report *Ontologies in the Behavioral Sciences: Accelerating Research and the Spread of Knowledge* will serve as the principal source document because many of the challenges it identifies in the behavioral sciences would also apply to competition and conflict.[43]

The process of building an ontology for the cognitive space involves several steps, beginning with the development of use cases and tool elements that help give it structure. These use cases and tool elements provide the concepts and dimensions one needs to understand cognitive warfare. Once these are established, the next steps involve defining classes, arranging them hierarchically, specifying their attributes or properties, and populating the ontology with instances and values. This process is iterative, allowing for constant refinement as the understanding of the cognitive domain evolves.

Photo: (Getty Images)

Use Cases

The NASEM use the term *use cases* within the context of software engineering to refer to situations in which software is usefully applied or to which it responds. It is a "narrative description or story involving someone interacting with a system to achieve a particular goal."[44] Use cases are crucial to building an ontology as they define its scope and identify key concepts by outlining specific needs and scenarios. They ensure the ontology's relevance and usability by focusing on the end-users' requirements. Additionally, use cases facilitate effective communication among stakeholders and guide the ontology's evaluation and validation, supporting an incremental development approach. The NASEM envisioned scenarios for what a system should do to help someone achieve a goal in a given context. These scenarios therefore differ from case studies, which represent fully realized instances of systems or applications.

The NASEM's use case model is a tool for designing their ontology. It illustrates use cases in terms of five parameters: (1) actors (2) behaving in a particular context who are (3) using a resource (4) to achieve an expected outcome (5) that may affect additional stakeholders (see table 1).

In the context of competition and conflict in the cognitive space, one might suggest the use cases in table 2 from which readers can begin to identify ontological elements.

The above use cases are designed to flesh out elements of an ontology of the cognitive space, but this is certainly not a comprehensive list. Below the report proposes a list of tool dimensions of the cognitive space, as the section above outlined based on the literature, to form a comprehensive framework for understanding the multifaceted nature of cognitive warfare. Each dimension delves into distinct aspects of cognitive threats and opportunities, revealing a complex landscape that adversaries and potential defenders must navigate. These are tools that one can employ or surveil in the use cases.

1. **Tools that leverage cognitive biases of individuals and their perception:** This dimension underscores the importance of exploiting inherent human cognitive biases and

Table 1. Five Parameters of a Use Case

ACTOR	CONTEXT	RESOURCE	EXPECTED OUTCOME	STAKEHOLDER
Anyone/anything who performs a behavior to put a demand on the resource or system	Set of conditions that must be true or present before the use case proceeds; constrains the use case	Any ontological entity, system, or object that the ontological entity proximally informs or enables	Goal state or preferred state of the actor	Any individual or entity with vested interest in the behavior of the resource or system under discussion or who may be affected by it
Example: researcher, health care provider, policymaker, general public	Example: workplace, hospital, online or mobile device, home, government office, "during a pandemic" or other broader context	Example: Resource Discovery System, a visualization tool, a knowledge graph, a search engine, automated data sets, standard set of terms and definitions, an ontology of behavioral science	Example: theory advancement, guidance on better sleep, financial management education for citizens	Example: public, patients, students, administrators, policymakers, law enforcement

Source: Based off of National Academies of Sciences, Engineering, and Medicine, *Ontologies in the Behavioral Sciences: Accelerating Research and the Spread of Knowledge* (Washington, DC: National Academies Press, 2022), https://doi.org/10.17226/26464.

Table 2. Cognitive Warfare Use Case Examples

ACTOR	CONTEXT	RESOURCE	EXPECTED OUTCOME	STAKEHOLDER
Military Planning Staff (Example: J5)	Combatant Command Headquarters Staff	Ontological list of concepts and relationships	Integration of cognitive operations into operational campaign plans	Combatant Commander; Joint Chiefs, Secretary of Defense
Counterintelligence	Department of Justice	Intelligence, surveillance, reconnaissance (ISR) application of the cognitive space	Detection and identification of cognitive campaigns being waged against the US	Public, law enforcement, political leadership, foreign intelligence targets
Strategic Communications	Interagency	Ontological influence relationship map	Foreign partners' alignment with US objectives through perception management	Foreign partner governments, global population, media, social media
Deception Planning Team	Combatant Command Joint Headquarters	Identification of key adversary influencers	Adversary operations or resource decisions that benefit US interests	Military forces, allied and coalition partners
Homeland Defense	Interagency	Ontological relationships between public and private entities	Resiliency and redundancy of critical infrastructure	Federal agencies, critical industries, general public

Source: Author.

perceptual vulnerabilities. Adversaries can manipulate the way individuals perceive information, making them more susceptible to false narratives, misinformation, or emotional appeals. These cognitive biases may include confirmation bias, anchoring, and cognitive dissonance, which adversaries can exploit to shape perceptions and influence behavior.

2. **Tools that leverage neuroscience and biology:** Leveraging advances in neuroscience and biology allows adversaries to explore both soft and hard weapons. On the softer side, this dimension can encompass the development of persuasive techniques rooted in an understanding of brain function and psychological responses. On the harder side, it may involve the creation of substances or technologies that directly affect neural processes or cause physical harm.

3. **Tools that leverage social psychology and group dynamics:** Social psychology and group dynamics are key factors in shaping behavior and opinions. Adversaries can exploit these principles to manipulate group dynamics, sow discord, or influence collective decision-making. Techniques may include stoking polarization, encouraging conformity, and creating a sense of identity or belonging.

4. **Tools that leverage techno-social applications (information to influence groups):** This dimension highlights the role of technology in cognitive warfare. Adversaries can exploit the vast array of information and communication technologies to disseminate narratives, engage in social engineering, or conduct information operations. This encompasses the use of social media, online communities, and other digital platforms to influence targeted groups.

5. **Tools that leverage information technology:** Information technology provides tools for adversaries to launch cyberattacks, disrupt critical infrastructure, and engage in disinformation campaigns. This dimension covers a broad spectrum of digital threats, from hacking and data breaches to the spread of false information, which can erode trust and societal stability.

Importantly, these tool dimensions also represent opportunities for the US and its allies and partners. By understanding the cognitive warfare landscape and the techniques that adversaries employ, these entities can develop countermeasures and mitigation concepts. Additionally, the insights they gain from cognitive warfare can inform strategies to conduct operations against adversaries, enhancing national security, resilience, and strategic advantage.

Furthermore, recognizing the overlap between these dimensions is essential. Analysts might categorize tools that leverage technology as similar to the Open Systems Interconnection (OSI) transport layer, while they might view tools using group dynamics as on the network layer. Cognitive threats are not mutually exclusive, and adversaries may employ strategies that leverage multiple categories simultaneously (so can the US and its allies). Acknowledging this complexity makes it possible to develop comprehensive strategies and epidemiological approaches that address cognitive warfare's intricacies and defend against a wide range of threats and challenges.

The following are example strategies that adversaries are employing in the cognitive space today:

- Capture and control of strategic resources critical to information technology
- Intellectual property theft and conversion
- Control of international governance institutions that regulate information technology
- Dominance of design standards and transfer protocols
- Reorganization and reform of the military
- Reflexive control strategies
- Population influence strategies
- Network reconnaissance operations
- Information system sabotage

These strategies seek to achieve end states such as information control or population control, social disruption in a target country, doubts in military assurance, an advantageous form of economic development, and capture of the information initiative. Table 3 displays three examples.

The proposed tool dimensions mentioned earlier significantly inform the development of an ontology of cognitive warfare. An ontology is a formal representation of knowledge that defines concepts and the relationships between them within a specific domain. In the context of cognitive warfare, these dimensions serve as fundamental building blocks for constructing an ontology that systematically categorizes and organizes the diverse aspects of this complex field. Here is how these tool dimensions contribute to the formation of a cognitive warfare ontology:

1. **Categorization of cognitive threats and opportunities:** The tool dimensions provide a systematic way to categorize cognitive threats and opportunities. Each dimension represents a distinct category of threat and opportunity, enabling the ontology to classify and differentiate the various strategies that adversaries employ. This categorization is essential to a structured understanding of the cognitive warfare landscape.
2. **Interrelationships:** The ontology should capture the interconnections and dependencies between these dimensions. For example, threats and opportunities that leverage cognitive biases may intersect with those that exploit social psychology and group dynamics. This interconnectedness highlights the complexity of cognitive warfare and illustrates how different dimensions may reinforce each other in adversarial strategies.

Table 3. Cognitive Warfare Strategy Examples

STRATEGY	VULNERABILITY	PAYLOAD	THREAT DIMENSION	MEDIUM	OBFUSCATION	TARGET	END STATE
Electronic deception	Reliance on over-the-horizon to find target	Malware delivered over radio frequency	Information technology, cognitive bias	Radar system	Malware hides in microprocessors	Radar system operator	Operator does not detect aircraft carrier
Reflexive control	American public self-segregates into information echo chambers	Compromised elite influencers	Social psychology, techno-social	Broadcast media, social media	Multiple elites driving same narrative, mainstream media bias toward "both sides"	Self-segregators	Lost trust in representative government institutions
Control over information strategic resources	Key resources have been off-shored to adversary control	Global markets moved through volume and price	Information technology	Critical spectrum components (routers, modems, satellites, chips, etc.)	Parent company headquarters located in US and "friendly" countries	Key defense and national security information systems	During crisis and conflict, key resources cut off

Source: Authors.

3. **Subcategories:** One can further subdivide each dimension to capture specific tactics, techniques, and procedures that the US and its allies or adversaries may use. For instance, under the dimension "Tools that leverage cognitive biases," subcategories may include confirmation bias, anchoring, availability heuristic, and more. These subcategories help in granularly defining the tactics involved.

4. **Mitigation and countermeasures:** The ontology can include a section on mitigation and countermeasures. This segment would outline strategies, tools, and techniques to counteract each dimension of cognitive threat and opportunity. Understanding how these countermeasures relate to the threat dimensions is critical for developing effective defense strategies.

5. **Dual-use nature:** Recognizing that the same dimensions represent both threats and opportunities is integral to the ontology. The ontology should illustrate how the US and its allies or adversaries can leverage each dimension for defense and strategic advantage. For example, advances in neuroscience can inform both defensive strategies against cognitive threats and the development of persuasive messaging techniques for influence campaigns.

6. **Technological and tactical overlaps:** Cognitive warfare frequently blurs the lines between traditional warfare and information warfare. Therefore, the ontology should highlight the overlap between technological threats and opportunities (e.g., information technology) and cognitive threats and opportunities. This overlap acknowledges the importance of cybersecurity and digital resilience in cognitive warfare.

7. **Dynamic nature:** The ontology should account for the dynamic nature of cognitive warfare. As new tactics and technologies emerge, the threat and opportunity dimensions evolve. The ontology should be flexible and adaptive to accommodate these changes and provide a framework for ongoing analysis and assessment.

In essence, the proposed tool dimensions serve as the foundational elements that enable the ontology to systematically organize, categorize, and interconnect the multifaceted aspects of cognitive warfare. They offer a structured approach to understanding this complex space, making it possible to identify, analyze, and respond to cognitive threats effectively. The resulting ontology becomes a valuable tool for military strategists, policymakers, and researchers to navigate the ever-evolving landscape of cognitive warfare and enhance national security.

Ontology Engineering Process

Having established use cases and tool elements to structure the ontology, this report will now turn to iteratively defining classes, arranging them hierarchically, specifying their attributes or properties, and populating the ontology with instances and values.

1. Classes in the cognitive domain

- Classes are fundamental concepts within the cognitive domain that represent collections of elements with similar properties or characteristics. This report uses these classes to categorize and organize various aspects of cognitive warfare. For instance, a class could be Information Operations, which encompasses a set of strategies and tactics.
- Classes often form a taxonomic hierarchy in which a superclass contains subclasses. This hierarchy allows for the organization of concepts in a structured manner. Using the example class Fruit, a subclass could be Apple, which inherits properties from the superclass.
- It is crucial to recognize that classes represent the underlying concepts in the domain, irrespective of a class's specific name. Synonyms for the same concept do not create separate classes. Including synonyms in class definitions enhances clarity and understanding.

2. Attributes and properties

- Each class has associated attributes or properties that describe aspects of that class. These properties can be intrinsic, extrinsic, parts, or relationships to other properties. In the context of the Fruit class, attributes might include Color, Taste, and Cultivation Climate.
- Properties can vary in complexity, ranging from simple attributes like Color to more complex ones that capture intricate relationships between elements in the ontology. Some properties may have constraints that define or limit their possible values. For example, the property Origin can have values like Florida Oranges or California Oranges to specify the specific farm or location where a fruit is grown.
- The attributes and properties associated with each class help provide a detailed and comprehensive understanding of the elements within the ontology.

3. Inheritance and multiple superclasses:

- Classes can have more than one superclass, allowing for flexibility in organizing and representing concepts. Subclasses inherit attributes, properties, and constraints from their parent classes, which contributes to the coherence and consistency of the ontology. For example, if Information Operations is a subclass of Cognitive Warfare Strategies, it inherits the properties and constraints associated with its superclass.

Building an ontology is a dynamic process, and it often involves collaboration and feedback from experts in the domain. As new knowledge and insights emerge, the ontology's developers can refine and expand it to capture the evolving understanding of cognitive warfare. The use of classes, properties, and hierarchies in ontology development provides a structured and systematic framework for comprehensively defining, organizing, and analyzing the cognitive domain and its various dimensions and elements.

Cognitive Warfare Ontology

To construct an ontology of cognitive warfare using the six top-level classes (Actor, Process, Space, Event, Tangible, and Intangible), one can map the proposed threat dimensions to these classes. This mapping allows for a structured representation of how these dimensions inform the ontology:

1. Actor class
   - **Threats that leverage cognitive biases of individuals and their perception:** This dimension primarily involves human actors (individuals or groups) who exploit cognitive biases. One can classify these actors in the Actor class, emphasizing their central role in cognitive warfare.
   - **Threats that leverage neuroscience and biology:** Here, actors may include scientists, researchers, or institutions working on applications of neuroscience and biology to warfare. These actors become part of the ontology in this dimension.

2. Process class
   - **Threats that leverage social psychology and group dynamics:** The Process class can encompass the strategies and methods used to exploit group dynamics. This includes the processes of group manipulation, persuasion, and social influence tactics.
   - **Threats that leverage techno-social applications (information to influence groups):** This dimension involves processes related to the use of technology and information to influence groups. One can categorize these processes, such as social media manipulation and targeted messaging campaigns, in this class.

3. Space class
   - **Threats that leverage information technology:** The Space class can represent the digital realm, where actors employ information technology. This space includes online platforms, networks, and communication channels that serve as battlegrounds for cognitive warfare.

4. Event class
   - **Threats that leverage cognitive biases of individuals and their perception:** Events in this dimension could include specific incidents or campaigns designed to exploit cognitive biases, such as disinformation campaigns or psychological operations.
   - **Threats that leverage neuroscience and biology:** Events may involve the development and deployment of neuroscientific technologies and interventions in warfare.

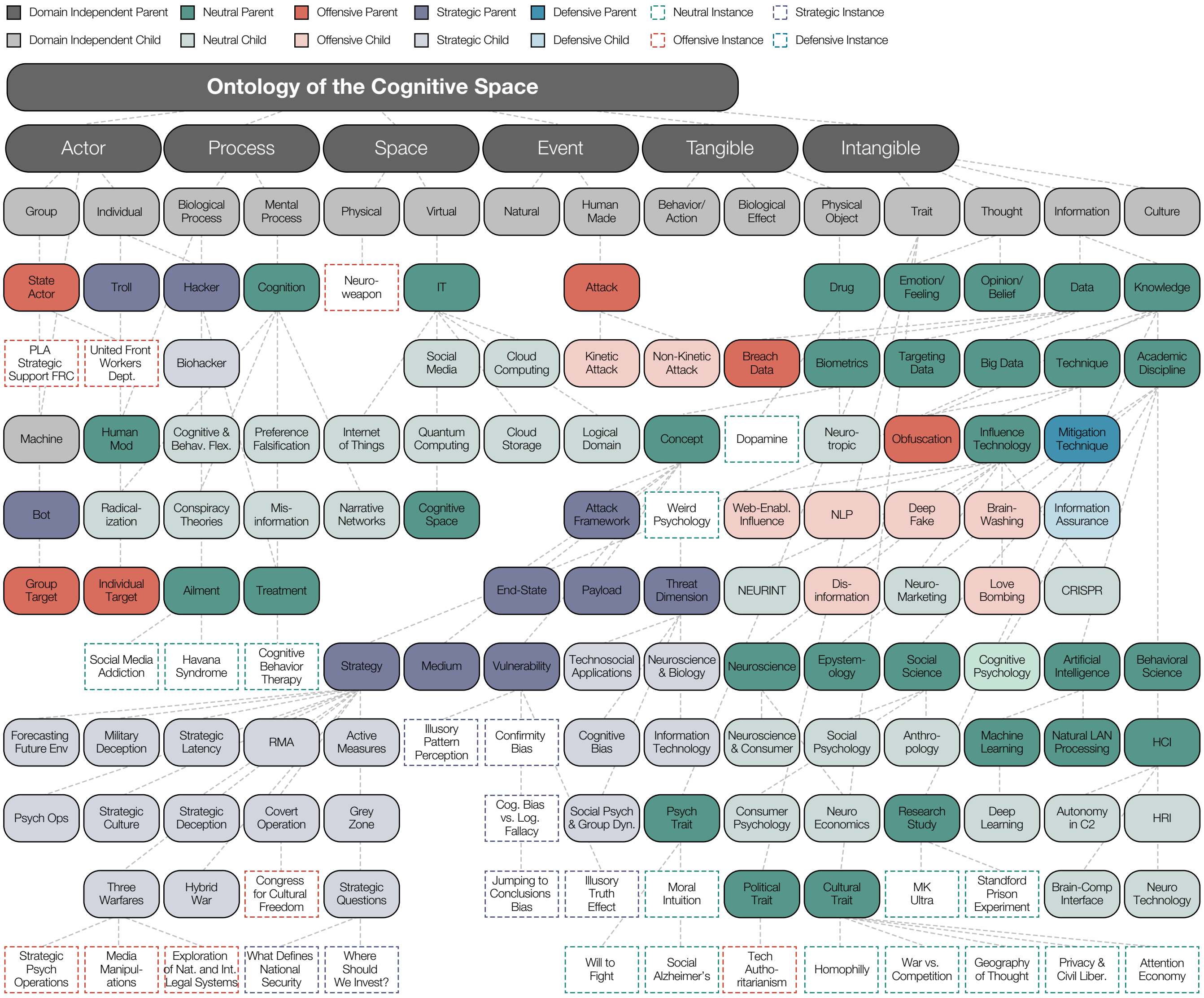
5. Tangible class
   - **Threats that leverage cognitive biases of individuals and their perception:** Tangible assets within this dimension can include physical materials, equipment, or tools that actors use in activities like propaganda distribution or deception tactics.
   - **Threats that leverage neuroscience and biology:** Tangible elements may involve physical devices or substances that affect the cognitive and neural processes of individuals.

6. Intangible class
   - **Threats that leverage social psychology and group dynamics:** Intangible aspects could include psychological manipulation, influence tactics, and the spread of ideas and beliefs through intangible means, like narratives and cultural influences.
   - **Threats that leverage techno-social applications (information to influence groups):** Intangible assets encompass digital content, information, and narratives disseminated through digital channels to influence group behavior.

Mapping the threat dimensions to the classes, this report proposes the initial ontology of the cognitive space, as depicted in figure 3.

Structuring the ontology in this manner aligns each threat dimension with one or more top-level classes, providing a comprehensive framework for understanding cognitive warfare. This approach allows for a systematic organization of actors, pro-

Figure 3. Ontology of the Cognitive Space



Source: Author.

cesses, spaces, events, tangible assets, and intangible aspects involved in cognitive warfare. Additionally, it highlights the interconnectedness between these dimensions, facilitating a holistic perspective of the field. The ontology aids in the identification of vulnerabilities, the development of countermeasures, and the assessment of opportunities in cognitive warfare.

CONCLUSION

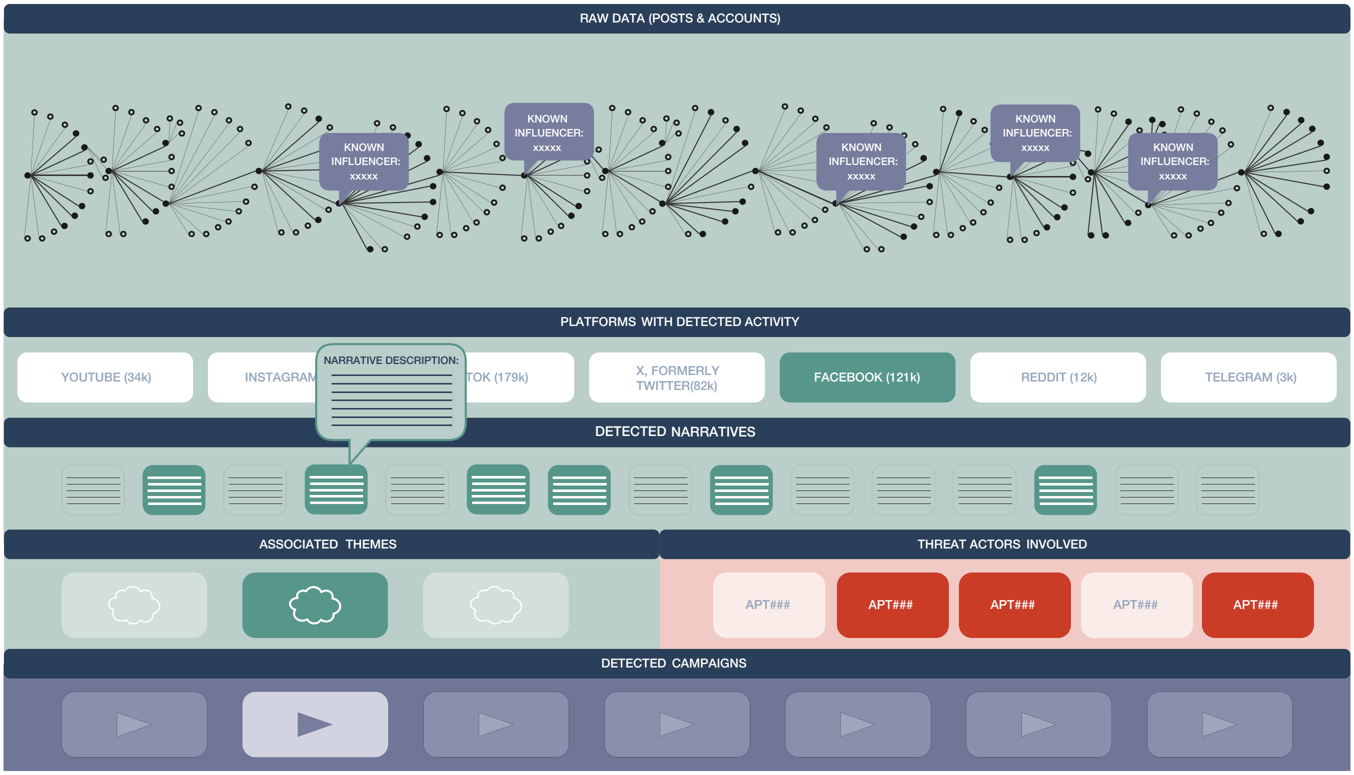
The proposed cognitive warfare ontology harnesses the power of three forces that are shaping the global security landscape. These forces, consisting of breakthroughs in neuroscience and synthetic biology, the exponential growth of dual-use technologies, and the influential role of algorithm-driven business and marketing techniques in shaping public behavior, have combined to create a multifaceted and dynamic cognitive space. By structuring this ontology around the six top-level classes—Actor, Process, Space, Event, Tangible, and Intangible—this report has categorized and addressed the intricate dimensions of cognitive warfare. This ontology allows decision-makers to analyze and understand the intricacies of cognitive threats that leverage these forces, providing insight into the contemporary security environment.

The cognitive warfare ontology can empower national security decision-makers with strategies and operational concepts tailored to cognitive competition. It supplies a framework within which they can assess and counter various threat dimensions. Decision-makers can employ this ontology to develop countermeasures against threats that exploit human cognitive biases, leverage cutting-edge technologies, or manipulate group dynamics. The tool helps in crafting both deliberate and response strategies.

In the effort to operationalize the cognitive space for national security, the next steps are critical. These entail the refinement and expansion of the ontology to accommodate evolving cognitive threats. Additionally, it is essential to integrate this on-

Photo: Photo: People try out augmented reality glasses at the booth of XREAL, Inc. during the Mobile World Congress (MWC) Shanghai 2023 on June 28, 2023, in Shanghai, China. (Photo by VCG/VCG via Getty Images)

Figure 4. Notional Sketch of a Visualization Display of a Cognitive Campaign



Source: Author.

tology into existing security protocols and practices, ensuring it becomes an indispensable part of threat assessment and response. Collaboration among experts from various fields—including psychology, technology, and security studies—is vital to refine the ontology and enhance its capabilities. Finally, it can serve as a foundation for the development of decision visualization models necessary for threat detection and opportunities for employment, as depicted in figure 4.

As the world ventures into the uncharted territory of cognitive warfare, several research questions loom. These questions encompass not only the technical aspects of ontology development but also the ethical and legal dimensions of cognitive warfare, as well as how the United States might need to organize for conflict in this space. How can the US protect the privacy and autonomy of individuals in an environment where cognitive manipulation is persistent? What are the legal boundaries of cognitive warfare, and how can international cooperation address this evolving problem? Furthermore, as cognitive threats become increasingly sophisticated, how can we fortify critical infrastructures against attacks that blend tangible and intangible elements in the cognitive space? Ultimately, how can the American polity ensure that its democratic system remains tenable?

As this new dimension becomes more prominent, the character of war and perhaps analysts' understanding of the entire conflict spectrum will continue to evolve. However, the impact of cognitive warfare may be significant. The world is likely at the beginning stages of the emergence as the three forces shaping the environment evolve at different rates. It is unclear how this variance may impact the dynamics of integrating advanced brain sciences, advanced technology, and algorithm-based attention models. States, nonstate actors, and the commercial sector are all engaged in a race of adaptation and innovation, developing and experimenting with new operational concepts. To address the impact on warfare, does the US need to consider how it is currently organized to compete in the cognitive space? If so, who are the key stakeholders, and might they be *outside* the traditionally understood national security ecosystem of the intelligence community and the DoD? What lessons might one draw from the past, perhaps from the Cold War, the national reorganization around the introduction of nuclear capabilities, and the resulting changes in the character of warfare? Does competition in the cognitive space require organizations to reevaluate human capital and how they recruit, train, develop, and employ it? How will cognitive warfare security requirements diffuse across not only the entirety of US government (federal, state, and local) but all of American society?

In sum, the proposed cognitive warfare ontology, informed by the forces shaping the global security environment, stands as a pivotal tool in America's arsenal. It equips national security decision-makers with the means to navigate the complexities of cognitive warfare, offering both a proactive stance against emerging threats and a reactive response to existing challenges. Yet as this realm continues to evolve, it is crucial to remain vigilant, adaptable, and forward-thinking. Only by addressing these future research questions and refining our approach can the US truly secure its cognitive spaces in an era defined by cognitive warfare.

ENDNOTES

[1] Andrew F. Krepinevich, *The Origins of Victory: How Disruptive Military Innovation Determines the Fate of Great Powers* (New Haven: Yale University Press, 2023).

[2] Information warfare employs the "battlespace use and management of information and communication technology in pursuit of a competitive advantage over an opponent." For the US Department of Defense, "information operations" are used in peacetime, while information warfare is used in conflict or war. It is closely related to military operations such as deception and psychological warfare. See "Information Warfare," Dictionary of Populism (blog), European Center for Populism Studies, accessed October 29, 2023, https://www.populismstudies.org/Vocabulary/information-warfare.

[3] Jeffrey Becker, "Joint Operating Environment 2040," Intelligence Knowledge Network (blog), 2020, https://www.ikn.army.mil/apps/MIPBW/MIPB_Features/Becker.pdf.

[4] National Academies of Sciences, Engineering, and Medicine, *Ontologies in the Behavioral Sciences: Accelerating Research and the Spread of Knowledge* (Washington, DC: National Academies Press, 2022), https://doi.org/10.17226/26464.

[5] Krepinevich, *The Origins of Victory*.

[6] Michael Warner and John Childress, *The Use of Force for State Power—History and Future* (Cham, Switzerland: Palgrave Macmillan, 2020).

[7] James Giordano, "Brain Science and Neuro-cognitive Warfare: Present and Future," PowerPoint presentation at Hudson Institute, 2023.

[8] David S. Alberts et al., *Understanding Information Age Warfare* (Washington, DC: DoD Command and Control Research Program, 2001); Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc., 2004).

[9] Bernard Claverie, Baptiste Prébot, Norbou Buchler, and Francois du Cluzel, eds., *Cognitive Warfare: The Future of Cognitive Dominance* (Bordeaux, France: NATO CSO STO, 2022), https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf; Francois du Cluzel, *Cognitive Warfare* (Norfolk, VA: Allied Command Transformation, 2021), https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf; Ajit Maan and Paul Cobaugh, *Introduction to Narrative Warfare* (Washington, DC: Narrative Strategies LLC, 2018); Robin Burda, *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds* (The Hague, Netherlands: The Hague Centre for Strategic Studies, 2023), https://hcss.nl/report/cognitive-warfare-as-part-of-society-never-ending-battle-for-minds.

[10] James Holly, *Influence and Perception Management Office*, Strategic Multilayer Assessment Conference, October 3, 2023, https://nsiteam.com/smaspeakerseries_03october2023; Lawrence A. Kuznar, *Modeling Exploitable Conditions in the 21st Century Strategic Environment*, AFOE Speaker Series, SMA Conference, November 30, 2022, https://nsiteam.com/modeling-exploitable-conditions-in-the-21st-century-strategic-environment; David Omand, Jonathan Moreno, and Jim Giordano, "Success and the Ethics of Harnessing Mind Plus Technology," panel moderated by Nicholas Wright, EUCOM Speaker Session, SMA Conference, 2022, https://nsiteam.com/success-and-the-ethics-of-harnessing-minds-plus-technology; Scott Atran, "The Minds and Actions of Devoted Actors and the Will to Fight: A Behavioral and Brain Studies Approach to War and Extreme Group Conflict," presentation at SMA Conference, September 12, 2023, https://nsiteam.com/smaspeakerseries_13september2023-2; Mick Ryan, William D. Casebeer, and David Huberdeau, "The Quantified Warrior: Monitoring the Physiology of the Human for War," presentation, Mind-Tech Nexus Series, SMA Conference, February 16, 2023, https://nsiteam.com/the-quantified-warrior-monitoring-the-physiology-of-the-human-for-war; Scott Atran, "Transcultural Predictors of Will to Fight," presentation, General Speaker Session, SMA Conference, October 12, 2022, https://nsiteam.com/transcultural-predictors-of-will-to-fight.

[11] "Information Operations," RAND, accessed April 9, 2024, https://www.rand.org/topics/information-operations.html.

[12] Jeffrey Becker, "Joint Operating Environment 2040."

[13] Zbigniew Brzezinski, *Between Two Ages: America's Role in the Technetronic Era* (New York: Viking Press, 1970), 12.

[14] Jonathan D. Moreno, *Mind Wars: Brain Research and National Defense* (New York: Dana Press, 2006).

[15] Joseph DeFranco, Diane DiEuliis, and James Giordano, "Redefining Neuroweapons: Emerging Capabilities in Neuroscience and Neurotechnology," *PRISM* 8, no. 3 (2019): 49–63.

[16] DeFranco, DiEuliis, and Giordano, "Redefining Neuroweapons"; James Giordano, "Battlescape Brain: Engaging Neuroscience in Defense Operations," *HDIAC Journal* 3, no. 4 (2016): 13–16; Diane DiEuliis, Charles D. Lutes, and James Giordano, "Biodata Risks and Synthetic Biology: A Critical Juncture," *Journal of Bioterrorism & Biodefense* 9, no. 1 (2018).

[17] James Giordano, Rohan Akhouri, and Dennis K. McBride, "Implantable Nano-Neurotechnological Devices: Consideration of Ethical, Legal, and Social Issues and Implications," *Journal of Long-Term Effects of Medical Implants* 19, no. 1 (2009): 83–93; Michael N. Tennison, James Giordano, and Jonathan D. Moreno, "Security Threat versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security," in *Neuroethics: Anticipating the Future*, ed. Judy Illes (Oxford: Oxford Academic, 2017), 531–53.

[18] DeFranco, DiEuliis, and Giordano, "Redefining Neuroweapons"; Diane DiEuliis and James Giordano, "Neurotechnological Convergence and 'Big Data': A Force-Multiplier toward Advancing Neuroscience," in *Ethical Reasoning in Big Data: An Exploratory Analysis*, eds. Jeff Collman and Sorin Adam Matei (New York: Springer, 2017); Giordano, "Battlescape Brain"; Celeste Chen, Jacob Andriola, and James Giordano, "Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China," in *Strategic Latency: Red, White, and Blue*, eds. Zachary S. Davis

and Michael Nacht (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2018), https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf.

[19] Elsa Kania, “Minds at War: China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology,” *PRISM* 8, no. 3 (2020): 82–101, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053585/minds-at-war-chinas-pursuit-of-military-advantage-through-cognitive-science-and.

[20] Nathan Beauchamp-Mustafaga, “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations,” China Brief (blog), September 6, 2019, https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations; Larry M. Wortzel, *Chinese Expectations for Biotechnology and Cognitive Enhancement in Future Warfare* (West Point, NY: Modern War Institute, 2022).

[21] Dean Cheng, *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017).

[22] Kerry K. Gershaneck, *Political Warfare: Strategies for Combating China’s Plan to “Win Without Fighting”* (Quantico, VA: Marine Corps University Press, 2020).

[23] Ross Andersen, “The Panopticon Is Already Here,” *The Atlantic*, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197.

[24] Jason Aten, “The Department of Defense Is Warning People Not to Use TikTok over National Security Concerns,” Inc., January 9, 2020, https://www.inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html; Jacqueline Deal and Eleanor Harvey, *CCP Weapons of Mass Persuasion* (Jaffrey, NH: Andrew W. Marshall Foundation, 2022), https://www.andrewwmarshallfoundation.org/library/ccp-weapons-of-mass-persuasion; Mack DeGeurin, “TikTok Leak Alleges User Data Isn’t Private: ‘Everything Is Seen In China,’” Gizmodo, June 17, 2022, https://gizmodo.com/tiktok-china-oracle-bytedance-1849078477; Sheridan Prasso, “China’s Tech Grip Persists in US Long after Orders to Rip It Out,” *Bloomberg*, May 11, 2022, https://www.bloomberg.com/news/articles/2022-05-11/us-ban-on-china-tech-failed-to-stop-use-of-hauwei-zte-hardware; Alyza Sebenius and Todd Shields, “Wireless Providers Serving Rural America Have a Huawei Problem,” *Bloomberg Businessweek*, April 22, 2020, https://www.bloomberg.com/news/articles/2020-04-22/wireless-providers-serving-rural-america-have-a-huawei-problem; Amanda Seitz, Eric Tucker, and Mike Catalini, “How China’s TikTok, Facebook Influencers Push Propaganda,” Associated Press, March 30, 2022, https://apnews.com/article/china-tiktok-facebook-influencers-propaganda-81388bca676c560e02a1b493ea9d6760; Patrick Tucker, “China’s Disinformation Warriors May Be Coming for Your Company,” *Defense One*, June 29, 2022, https://www.defenseone.com/technology/2022/06/chinas-disinformation-warriors-may-be-coming-your-company/368791; Yaqiu Wang, “WeChat Is a Trap for China’s Diaspora,” *Foreign Policy*, August 14, 2020, https://foreignpolicy.com/2020/08/14/wechat-ban-trump-chinese-diaspora-china-surveillance.

[25] Herbert Romerstein, “Disinformation as a KGB Weapon in the Cold War,” *Journal of Intelligence History* 1, no. 1 (2001): 54–67; Elizabeth Gibney, “Where Is Russia’s Cyberwar? Researchers Decipher Its Strategy,” *Nature*, March 17, 2022, https://www.nature.com/articles/d41586-022-00753-9; Margarita Levin Jaitner, “Russian Information Warfare: Lessons from Ukraine,” in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Talinn, Estonia: NATO CCD COE, 2015); Sam Bendett, Rita Konaev, and Chris Meserole, “Russian Integration of Humans and Technologies for Future War—Strengths and Vulnerabilities,” presentation, Mind-Tech Nexus Series, SMA Conference, November 3, 2022, https://nsiteam.com/russian-integration-of-humans-and-technologies-for-future-war-strengths-and-vulnerabilities.

[26] Bilyana Lilly, *Russian Information Warfare: Assault on Democracies in the Cyber Wild West* (Annapolis, MD: Naval Institute Press, 2022).

[27] Coco Feng, “Chinese President Xi Jinping Seeks to Rally Country’s Scientists for ‘Unprecedented’ Contest,” *South China Morning Post*, May 21, 2021, https://www.scmp.com/news/china/politics/article/3135328/chinese-president-xi-jinping-seeks-rally-countrys-scientists.

[28] Robert J. Bebber, “Treating Information as a Strategic Resource to Win the ‘Information War,’” *Orbis* (Summer 2017): 394–403.

[29] Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W.W. Norton & Company, 2023).

[30] Bill Gertz, *iWar: War and Peace in the Information Age* (New York: Threshold Editions, 2017).

[31] Scharre, *Four Battlegrounds*.

[32] Krepinevich, *Origins of Victory*.

[33] Rina Raphael, “Netflix CEO Reed Hastings: Sleep Is Our Competition,” *Fast Company*, November 6, 2017, https://www.fastcompany.com/40491939/netflix-ceo-reed-hastings-sleep-is-our-competition.

[34] Michela Balconi and Martina Sansone, “Neuroscience and Consumer Behavior: Where to Now?,” *Frontiers in Psychology* 12 (2021), https://doi.org/10.3389/fpsyg.2021.705850; Chen, Andriola, and Giordano, “Biotechnology, Commercial Veiling, and Implications.”

[35] “What Is Financial Technology (FinTech)? A Beginner’s Guide,” Columbia Engineering Boot Camps (blog), 2020, https://bootcamp.cvn.columbia.edu/blog/what-is-fintech; “What Is Digital Economy? Unicorns, Transformation and the Internet of Things,” Deloitte, 2023, https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html; Eben Harrell, “Neuromarketing: What You Need to Know,” *Harvard Business Review*, January 23, 2019, https://hbr.org/2019/01/neuromarketing-what-you-need-to-know; Lexie Kane, “The Attention Economy,” Nielsen Norman Group, June 30, 2019, https://www.nngroup.com/articles/attention-economy.

[36] Uma R. Karmarkar and Hilke Plassmann, “Consumer Neuroscience: Past, Present and Future,” *Organizational Research Methods* 22, no. 1 (2019): 174–95, https://doi.org/10.1177/1094428117730598; Peter H. Kenning and Hilke Plassmann, “How Neuroscience Can Inform Consumer Research,” *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 16, no. 6 (2008): 532–38, https://doi.org/10.1109/TNSRE.2008.2009788; Maureen Rhemann, *What We’ve Learned from 20 Years of Techno-Financial Intelligence* (Houston, TX: Reperi Analysis Center, 2020).

[37] Stefan Stieger and David Lewetz, “A Week without Using Social Media: Results from an Ecological Momentary Intervention Study Using Smartphones,” *Cyberpsychology, Behavior and Social Networking* 21, no. 10 (2018): 618–24, https://pubmed.ncbi.nlm.nih.gov/30334650/; “Teens and Social Media Use: What’s the Impact?,” Mayo Clinic, December 21, 2019, https://www.mayoclinic.org/healthy-lifestyle/tween-and-teen-health/in-depth/teens-and-social-media-use/art-20474437; Mary Aiken, *The Cyber Effect* (New York: Spiegel & Grau, 2016).

[38] *Aiken, The Cyber Effect;* “The Top Mental Health Challenges Facing Students,” Best Colleges, 2020, https://www.bestcolleges.com/resources/top-5-mental-health-problems-facing-college-students.

[39] Brendan Helm and Dina Smeltz, “OK, Boomer: Youth Hesitant to Use Force, Shun US Exceptionalism in Foreign Policy,” Chicago Council on Global Affairs, February 4, 2020, https://globalaffairs.org/research/public-opinion-survey/ok-boomer-youth-hesitant-use-force-shun-us-exceptionalism-foreign.

[40] Aten, “Department of Defense Is Warning People Not to Use TikTok”; DeGeurin, “TikTok Leak Alleges User Data Isn’t Private”; Seitz, Tucker, and Catalini, “How China’s TikTok, Facebook Influencers Push Propaganda”; Wang, “WeChat Is a Trap for China’s Diaspora”; Sebenius and Shields, “Wireless Providers Serving Rural America Have a Huawei Problem”; Prasso, “China’s Tech Grip Persists in US.”

[41] Kane, “The Attention Economy”; “Paying Attention: The Attention Economy,” *Berkeley Economic Review*, March 31, 2020, https://econreview.berkeley.edu/paying-attention-the-attention-economy.

[42] Lucina Q. Uddin, “Cognitive and Behavioral Flexibility: Neural Mechanisms and Clinical Considerations,” *Nature Reviews* 22 (2021): 167–79; Jan-Willem van Prooijen, Karen M. Douglas, and Clara De Inoncenio, “Connecting the Dots: Illusory Pattern Perception Predicts Belief in Conspiracies and the Supernatural,” *European Journal of Social Psychology* 48, no. 3 (2018): 320–35, https://onlinelibrary.wiley.com/doi/full/10.1002/ejsp.2331; Jonathan Haidt and Tobias Rose-Stockwell, “The Dark Psychology of Social Networks,” *The Atlantic*, December 2019, https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763; Jonathan Haidt, “Yes, Social Media Really Is Undermining Democracy,” *The Atlantic*, July 28, 2022, https://www.theatlantic.com/ideas/archive/2022/07/social-media-harm-facebook-meta-response/670975; Dan Kahan et al., “Motivated Numeracy and Enlightened Self-Government,” *Behavioural Public Policy* 1, working paper 307 (September 8, 2013): 54–86, https://doi.org/10.2139/ssrn.2319992; Drew Westen et al., “Neural Bases of Motivated Reasoning: An fMRI Study of Emotional Constraints on Partisan Political Judgement in the 2004 US Presidential Election,” *Journal of Cognitive Neuroscience* 18, no. 11 (2006): 1947–58.

[43] National Academies of Sciences, Engineering, and Medicine, *Ontologies in the Behavioral Sciences: Accelerating Research and the Spread of Knowledge* (Washington, DC: National Academic Press, 2022), https://nap.nationalacademies.org/catalog/26464/ontologies-in-the-behavioral-sciences-accelerating-research-and-the-spread.

[44] *Ontologies in the Behavioral Sciences*, 18.

Notes

Hudson Institute
1201 Pennsylvania Avenue, NW, Fourth Floor, Washington, DC 20004
+1.202.974.2400 www.hudson.org