Marine Corps Lance Corporal Jackson Wilkie, defensive cyberspace warfare operator with Delta Company, 3rd Radio Battalion, III Marine Expeditionary Force Information Group, monitors enterprise network for digital threats, Marine Corps Base Hawaii, April 8, 2024 (U.S. Marine Corps/Bridgette Rodriguez)

Cognitive Warfare

The Fight for Gray Matter in the Digital Gray Zone

By Michael J. Cheatham, Angelique M. Geyer, Priscella A. Nohle, and Jonathan E. Vazquez

The sphere of operations will expand from the physical domain and the information domain to the domain of consciousness; the human brain will become a new combat space.

—He Fuchu, Vice President of the PLA's Academy of Military Sciences[1]

The United States is facing unprecedented challenges in the cognitive domain. While democracies struggle to develop frameworks that promote collective understanding, adversaries are employing *gray zone* tactics—those that never rise to the level of war—as a form of cognitive warfare against the United States and other democratic societies. François du Cluzel, head of innovative projects at the North Atlantic Treaty Organization (NATO)'s Allied Command Transformation Innovation Hub, describes the key distinctions of the emerging cognitive domain:

Cognitive warfare degrades the capacity to know, produce, or thwart knowledge. Cognitive sciences cover all the sciences that concern knowledge and its processes (psychology, linguistics, neurobiology, logic, and more).

Cognitive warfare is, therefore, the way of using knowledge for a conflicting purpose. In its broadest sense, cognitive

Lieutenant Colonel Michael J. Cheatham, USAF, is Deputy Director of the Joint Staff Security Office. Commander Angelique M. Geyer, USCG, is Chief of the Operational Planning Section at the U.S. Coast Guard Atlantic Area. Lieutenant Colonel Priscella A. Nohle, USA, is a Future Warfare Strategist at NATO Allied Command Transformation. Lieutenant Colonel Jonathan E. Vazquez, USAF, is the Collection Management Branch Chief and Asia-Pacific Chief Collection Planner in the Joint Staff J26 Deputy Directorate.

Marines and civilians with Marine Corps Cyberspace Warfare Group and Marine Corps Cyberspace Operations Battalion participate in Cyber Flag 23-2 at undisclosed location, August 7, 2023, to enhance readiness and cyber warfare capabilities (U.S. Marine Corps/Oneg Plisner)

warfare is not limited to the military or institutional world. Since the early 1990s, this capability has tended to be applied to the political, economic, cultural, and societal fields.

Any user of modern information technologies is a potential target. It targets the whole of a nation's human capital.[2]

The use of cognitive warfare to target "a nation's human capital" highlights a growing threat vector. *Cognitive warfare* aims to create cognitive-emotional conflict by influencing a target population's thoughts and values using technical means and information. As a target, human capital is a weak point in a nation's defense, particularly for nations that are highly connected and based on open systems. The brain's tendency to accept disinformation exposes a risk that affects a nation's defense and its broader society. The brain operates on the principle of survival. When individuals interpret inputs as threatening (actual or perceived), the brain's fear centers activate, executive-function areas cloud, and rational decision cycles are interrupted.[3]

Advertisers and media outlets recognize the brain's vulnerabilities and aggressively stimulate instinctual impulses to attract consumers and sell products. Similarly, strategic competitors, particularly Russia and China, leverage these same impulse pathways to shape the values and opinions of an external populace to confuse, polarize, and undermine a nation's governmental operations and planning processes.

Hardwired impulses, coupled with the brain's natural development and integration, leave us susceptible to thinking traps (that is, confirmation bias) and further exacerbate potential effects. *Confirmation bias* occurs when people search for and embrace information that reinforces currently held beliefs. Under threat, people commonly seek information to confirm their beliefs, and it becomes harder to change their minds later—even with updated and credible information.[4]

Strategic competitors recognize that saturating the information space with disinformation preys on the brain's "wetware" to believe and confirm. Saturation tactics with "sticky" information, familiar topics, and partial truths establish priming conditions for new shaping narratives to take hold. Russia and China are weaving these cognitive warfare tactics into their doctrines and are using instruments of national power to target the U.S. military and civilian populations.[5]

The Cognitive Domain

The Department of Defense (DOD) must consider the cognitive domain's technological and human components while developing tactics, techniques,

and procedures to recognize and defend within it. Offensively, U.S. Cyber Command maintains operations in the technological and human domains through information and psychological operation functions. Concurrently, DOD Information Network defense and annual cyber security training are part of defensive operations. However, DOD lacks a tangible corresponding protective function to support cognitive domain security.

There is an investment gap at the joint force level. Offensive and defensive components are parts of cognitive warfare, and technological and human elements nest within each (figure 1). The defense mechanism must be ingrained across the range of military operations, regardless of time, location, or operational standing. Defending the cognitive space of military personnel is paramount to the United States retaining its relative strategic advantages. Psychological and information lines on the human side of cognitive security (that is, the defense) are immediately necessary to defend U.S. military personnel actively and passively against cognitive warfare.

While technology is the preferred focus for delivering and defending capabilities in the information and cyber domains, joint force leaders must also consider human cognition as a primary concern. Cognitive warfare delivers effects through the cyber and information domains. In a highly interconnected operational environment, no domain exists in isolation.

Cognitive Warfare Adversaries

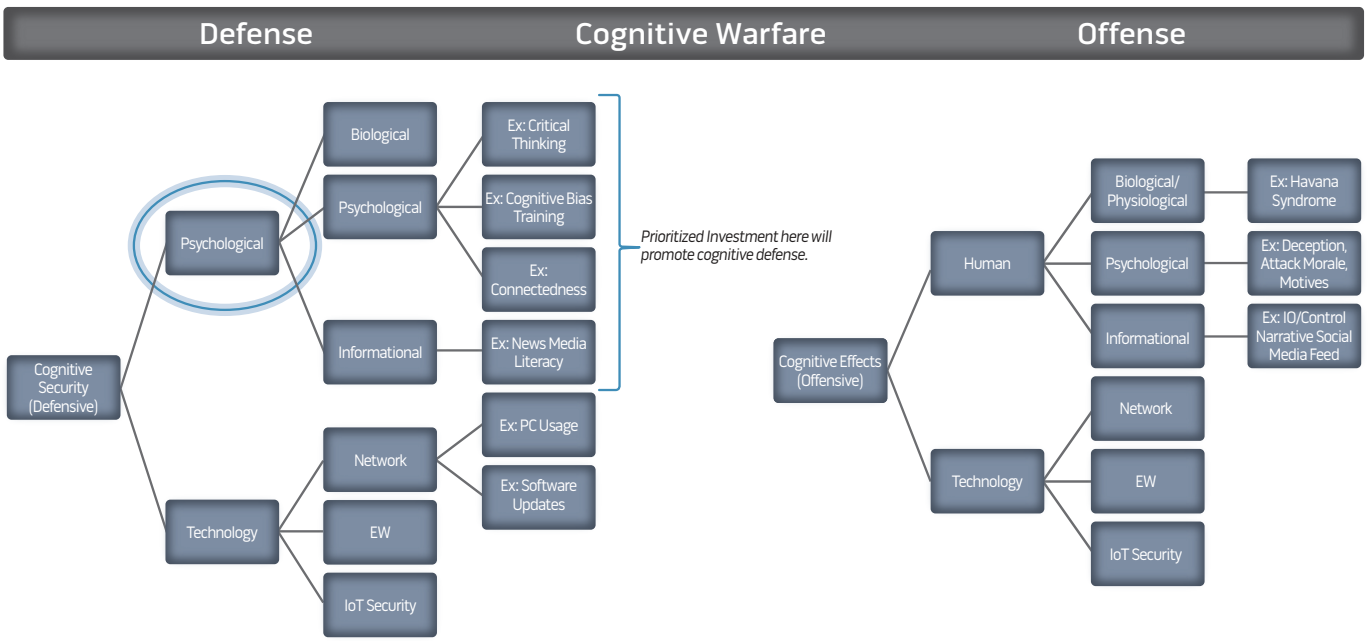
Today's strategic competition differs from past approaches. The Cold War, defined by a race for significant gains and overwhelming dominance, is over. Conventionally, the United States maintains a relative strategic advantage; the risk of Russia or China losing to the United States in a decisive conventional battle is high. In response, adversaries attempt to hijack the softer moral factors of target populations, making small gains and incrementally nudging progress across time and space. Altering how populations interpret what is occurring globally is the initial phase in changing reactionary outputs while concurrently gaining incremental progress.

Russia's Advantage in the Cognitive Domain. Russia employs a primary cognitive warfare tool rooted in perception manipulation control, known as *reflexive control*. Russian theory leverages reflexive control from the tactical to the strategic level. Its power potential broadens as technology and communication speeds grow. For the past 30 years, Russia has used the *maskirovka* (deception) technique, which provokes a chaotic response in the population by shaping information and public perception through disinformation tactics.[6]

Russia's disinformation warfare aims to avoid kinetic operations by masking attribution tactics, such as posing as U.S. organizations or individuals within the information and cyber domains.[7] The approach advocates for gray zone military operations to deliberately cloud the understanding between Russian and Western definitions of war. Western nation-states that narrowly frame war as kinetic-based must understand that this perspective is self-imposed. With this narrow framing, democratic nations fail to get to know their enemy and themselves.

Russia's influence during the 2016 U.S. Presidential campaign favoring then-candidate Donald Trump exemplifies a recent and significant cognitive warfare attack against a democratic nation and its population.[8] Russian attacks exploited freedom-of-speech ideals to undermine

Figure 1. Cognitive Warfare Defense and Offense



Source: Priscella A. Nohle

the U.S. electoral process. Facebook, Twitter, YouTube, and other social media sites, including those within Russia, spread disinformation about the opposing candidate, Hillary Clinton, to undermine the electoral process. Preceding the 2014 invasion of Crimea and the 2022 invasion of Ukraine, Russian President Vladimir Putin expanded his disinformation targeting to the global audience, attempting to justify and legitimize Russia's actions.[9] Russia (like China) also leverages state-run broadcasting organizations to influence foreign countries with false narratives and distort how Western populations interpret world events.[10]

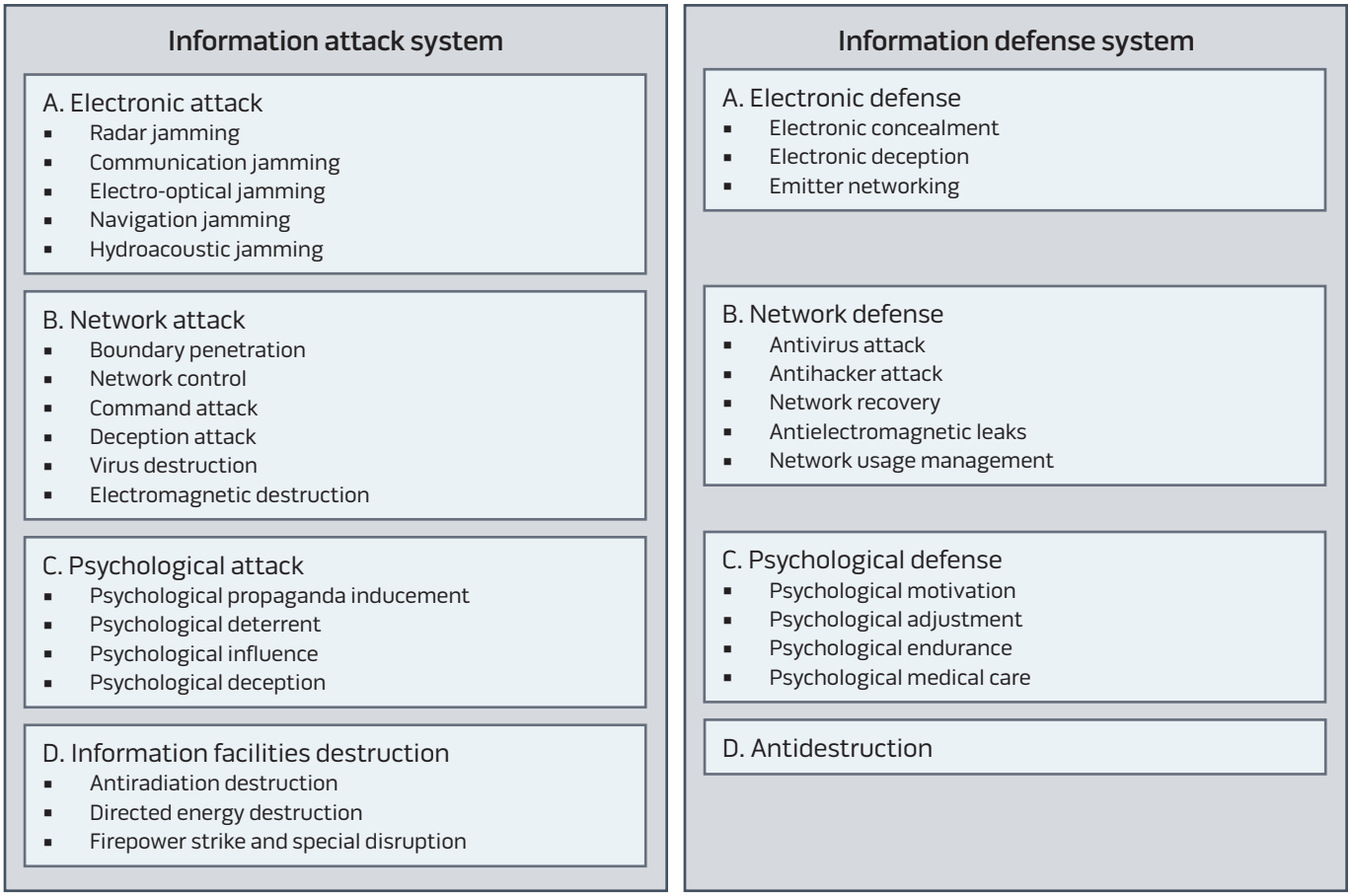
China's Posture to Conduct Cognitive Warfare. China favors an integrative approach to cognitive warfare known as the Information Confrontation System, which places psychological activities alongside network, electronic, and information systems attacks.[11] It includes propaganda, deterrence, influence, and deception as additional tools. Much like Russia, China views warfare as a constant state of competition across the implementation of all instruments of national power. Increased awareness and understanding should enable DOD to identify malign behaviors such as cyber data theft, election influence, and other attacks that aim to affect its personnel's cognitive space.[12]

Understanding the interrelationships of how people define spatial organization and interests will be as important as understanding how physical terrain shapes movement during military operations. This is known as human geography mapping, a potential core competency that requires further analysis. China's People's Liberation Army (PLA) embeds human geography understanding within its doctrine. Psychological reconnaissance enables measuring the effects of its psychological operations on various populations.[13] These tactics are part of China's overarching reconnaissance intelligence system, including electronic and network reconnaissance (figure 2).[14]

The PLA conducts offensive and defensive operations to assess its military's psychological motivation, preserve psychological health, build endurance for stressful situations, and provide immediate care for psychological trauma when needed. Defending against attacks in the cognitive domain is a crucial part of the PLA's Information Confrontation System. In contrast, the U.S. military does not integrate cognitive domain defense as part of its operations but treats it individually, as a medical support reaction.

China's strategic competition methods blend Western ways of warfare with

Figure 2. Chinese Information Confrontation System



Source: Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RR-1708-OSD (Santa Monica, CA: RAND, 2018), figure 3.7.

Airmen of 16th Air Force perform command and control of 16th Air Force Forces in 616th Operations Center, Joint Base San Antonio–Lackland, Texas, November 22, 2023 (U.S. Air Force/Sharon Singleton)

actions in the information, political, and economic space.[15] These actions complicate the U.S. ability to defend against attacks, as the battlespace is undefined, persistent, and continuous. This dynamic promotes the need for cognitive defense as a baseline skill set for every member of the joint force.

The Digital Gray Zone

Cognitive warfare is a subtle yet effective tool in the digital information environment. The rising trend of the Internet of Things and the speed of information access create unprecedented digital immersion for even the most modest embracers of technology. Digital immersion, in turn, changes how people process information. Rather than reading in a typical linear motion, eyes dart quickly across posts and pages from trustworthy and disreputable sources, searching for pertinent headlines to consume as truth.[16] The now-standard search for "quick hits" of information bits from headlines and social media comes at significant risk to the reader—a risk that Russia and China are deliberately embracing. Disinformation bits—deliberately distributed and processed at first glance, consciously and unconsciously—present unique challenges at the joint force level and unpredictable threats at an individual level.

Digital gray zone tactics like those used in 2020 highlight a critical joint force challenge. Following the George Floyd tragedy, a significant amount of all the tweets and Facebook postings related to that event were traceable to Chinese- and Russian-based accounts.[17] These state-sponsored postings deliberately stoked the passions of the U.S. population as a part of a calculated equation. Disinformation, coupled with an amplification of passion, served as an effective strike against the most vulnerable and strategic U.S. center of gravity—the strategic narrative.

The narrative space is a strategic center of gravity—the source of power or strength that enables a nation to achieve its aim—for any democratic-based government, especially the United States.[18] Since Russia and China are unlikely to win a decisive conventional victory against the United States today, they pursue a strategy to inflict a "functional defeat." Rather than seeking to conquer territory or destroy forces, they seek

to destroy the moral factors that drive the ability to resist. In a democracy, the people's will is the driver of power. When confusion and distrust prevail in the minds of an increasing number of people, the power equation shifts, and ideological parity becomes a closer reality—without firing a shot.

The Gray-Matter Zone

The brain operates in a neurosequential and iterative input-interpretation-output loop.[19] The loop supports predictability and certainty in the individual's interpretation of the world, increasing the odds of survival. However, disinformation creates a "low-resolution" understanding of what is occurring in the environment and how to respond. When uncertainty enters an individual's input-interpretation-output loop, the brain seeks to find further information to crosscheck against the information gap, confirmation bias ensues, and a disinformation loop follows. Figure 3 highlights the iterative assessment-reassessment cycle essential to shaping a personal narrative.

Individuals develop their personal narratives through experiences, beliefs, introspection, and what others think of them. When disinformation permeates internal beliefs and prevents a clear "mental map" of an individual's space and time, personal narratives are vulnerable to change. The brain's stress systems engage because a threat is present (that is, low-resolution mental maps show perceived threats to survival), and hypervigilance arises. Exposure to disinformation and hypervigilance over extended periods can warp a person's sense of self and structure of being. Naïveté of the cognitive warfare problem predisposes individuals to increased cognitive dissonance, which can express itself in unpredictable ways such as anger, disillusionment, nihilism, and sometimes self-harm.[20]

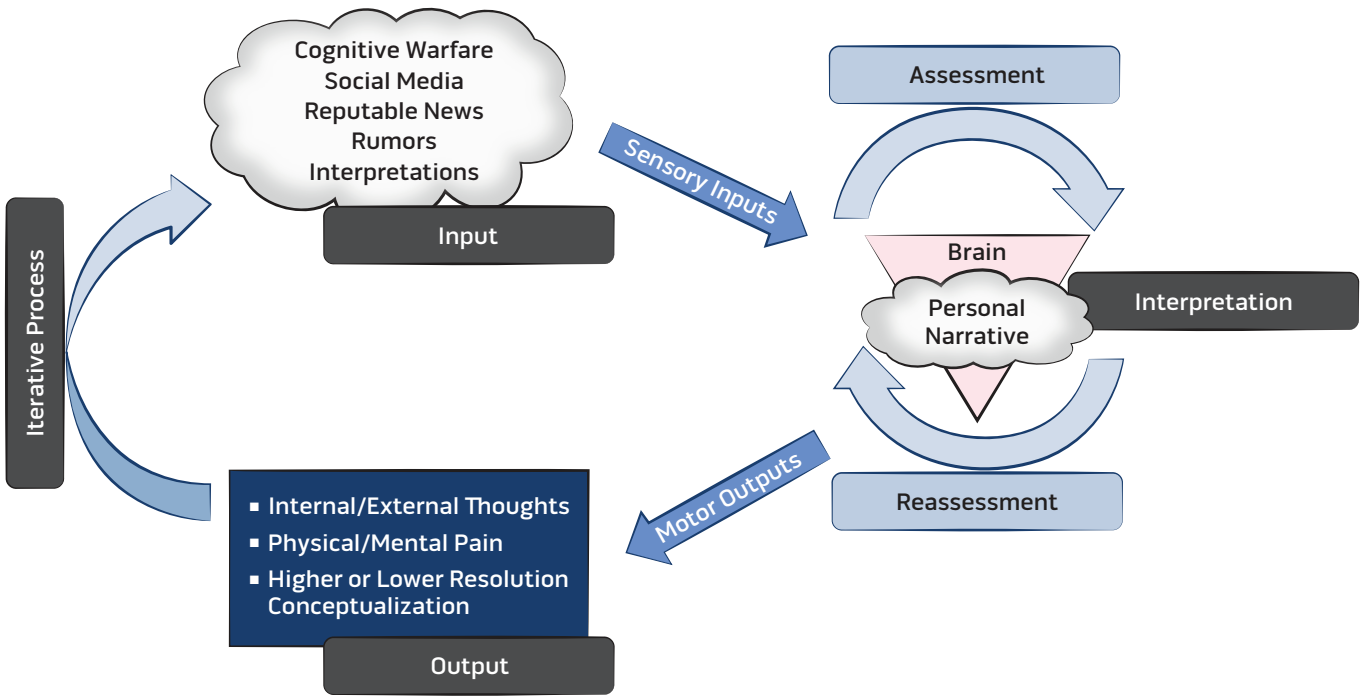
Awareness Precedes Change

Developing countermeasures to defend against cognitive warfare is possible, but it requires a baseline awareness that a problem exists. The Stages of Change Model asserts that a step-by-step process is essential to moving individuals from a current behavior state to the desired one.[21] Figure 4 highlights the significance of the first two steps to create change in cognitive warfare: precontemplation and contemplation.

An individual's awareness and reluctance to change often limit how much organizational systems can change. The current cognitive warfare environment indicates that many joint force personnel operate in *precontemplation*. In this stage, organizations and individuals are either unaware that a problem exists or do not acknowledge that it requires a strategic approach—they are not ready for change.[22] Defining and creating awareness of the problem promotes a shift from precontemplation to contemplation.

The *contemplation* phase of change begins once the organization and individuals realize that a problem exists and initiate thinking about taking steps toward action.[23] This phase is the process of taking those steps. The critical point in the contemplative phase is how organizations or individuals interpret change. If the idea of change is externally overpressurized, a feeling of potential threat arises, causing the organization and individuals to return to the earlier state

Figure 3. Personal Narrative Processing



Source: Michael J. Cheatham

(that is, denial) as a means of certainty, predictability, and survival. Therefore, the organization or individual must *internally* drive the idea of change. The drivers for change must support the organization's or individual's narratives so that each internalizes the understanding that cognitive warfare is happening now, and each is at risk. Developing the skills to think and operate beyond the baseline survival level—while consistently processing information in the executive-function areas of the brain—offers the greatest potential for resilience against the effects of cognitive warfare.

Recommendations

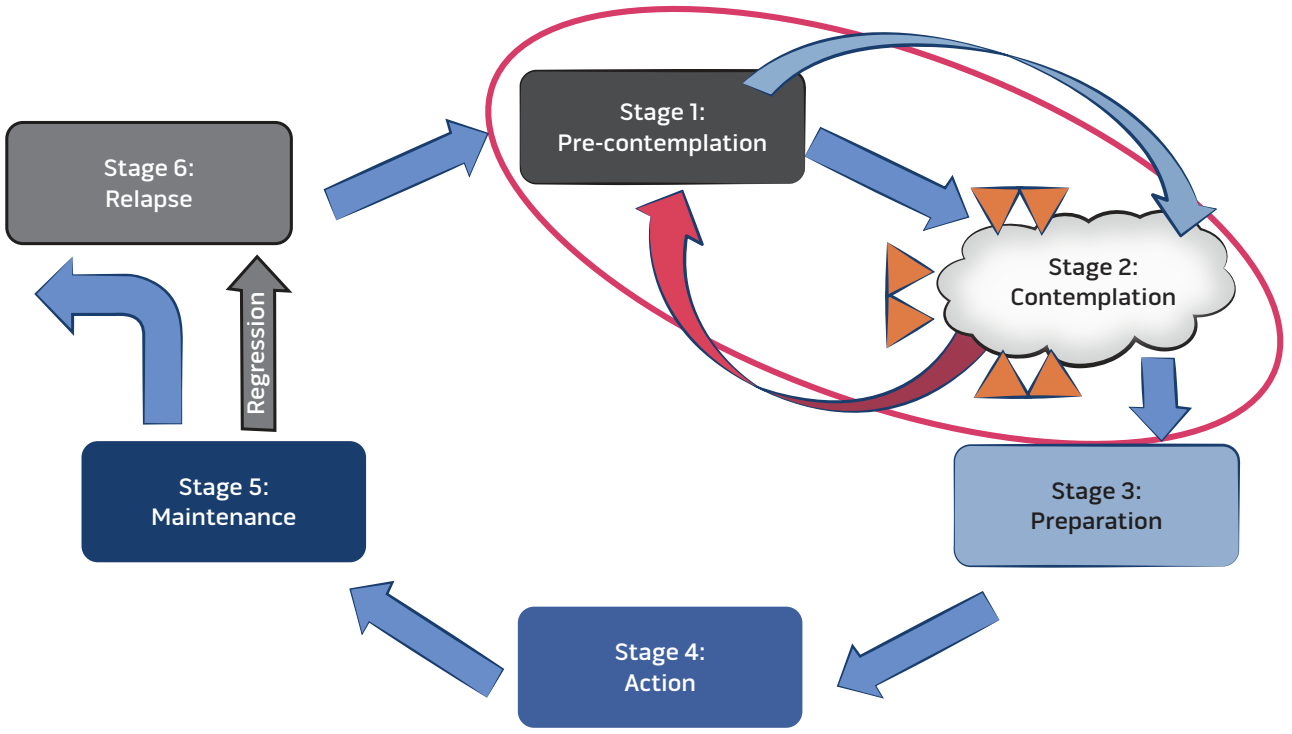
Cognitive security must begin with a basic standard of resilience in deciphering facts from opinions. Recent research indicates that individuals with high levels of political awareness and digital savvy are harder to penetrate mentally by narrative-based cognitive warfare.[24] Those individuals can distinguish fact from opinion with a higher success rate. Therefore, they are more likely to identify misinformation and avoid negative responses. Their "mental armor" is intact. Expanding the cognitive-security concept across the joint force is a crucial step. A cognitive-security strategic approach incorporates three primary lines of effort (LOEs).

LOE 1: Joint Force Leaders, Education, and Life Cycle Service Training. Through the Joint Staff, DOD should codify cognitive warfare as a domain for which the brain is the critical vulnerable target and dominant cognitive influence is the goal. Integrating the cognitive domain into joint doctrine will drive leaders to prioritize resources and emphasize domain competition. Concurrently, DOD must identify the implications of technology and information operations on individual cognitive abilities to process data and make decisions, then prioritize cognitive resilience as a weapon system.

DOD should include cognitive warfare training at every echelon of military training—beginning with basic training, at formal professional military education levels, and as part of routine annual training at the base level. Training should educate members on how information shapes thinking and how confirmation bias influences decisionmaking. Moreover, leaders must actively inform their members of the impacts of technology, social media–induced recency bias, and social spoofing (mimicking and affirming others' actions and beliefs to fit into one's social group) in their decisionmaking process. Leaders must remain proactive and build their personnel's ability to defend themselves from current attacks by facilitating training, such as mindfulness, cognitive reappraisal techniques, and actions to promote belonging and cohesion.

DOD should direct Service branches to include cognitive warfare defense-mechanisms training in existing resilience programs. Preemptively exposing Servicemembers to mental fitness and resilience skills training can also improve resilience in the cognitive domain.[25] Rather than relying only on highly educated and credentialed health professionals, trained tactical-level leaders should increasingly lead training. Tactical-level integration increases flexibility, lowers costs, and creates buy-in from those who most need the training.[26]

Figure 4. Stages of Change Model



Source: Michael J. Cheatham

LOE 2: Critical Media Literacy. Saturating the information environment with disinformation can produce information-learned helplessness.[27] Passive attacks are most successful against individuals already dealing with depression, low self-esteem, and pessimistic attitudes. Current research indicates that approximately 15 percent of the U.S. military population aligns with these risk categories.[28] To defend against these attacks, leaders should consider increasing critical and digital media literacy training programs to develop reasoning and interpretation techniques.

Findings from RAND, IREX, and Harvard University suggest that initial exposure to literacy videos and training decreased the likelihood of engaging with and spreading false information, and that this exposure significantly reduced the effectiveness of deliberately manipulated information.[29] The intent is to make already existing information and educational material available while bringing awareness to the problem and highlighting the benefits of media literacy. Critical media literacy material exists from available resources implemented across the civilian sector, such as the Florida education system's Cyber Florida project.[30] Training should be made available through formal and informal continuous training programs and military support organizations. Critical media and digital literacy build self-efficacy in navigating media and increase one's ability to identify credible information.[31]

LOE 3: Developing Defensive Mechanisms. Technology can help identify patterns and attribute disinformation from adversaries that seek to shape a particular message.[32] Similarly, by using artificial intelligence and machine learning, DOD can develop defensive tools to help military leaders disrupt adversaries' attempts to inject false information into public forums. An example is using artificial intelligence "to identify social media bots through automated 'bot spotting' or 'bot labeling'" to help detect fake social media accounts spreading disinformation.[33] Artificial intelligence may also aid as an educational tool by highlighting disinformation manipulation attempts and countering with techniques to avoid it in the future.[34]

Zhanna Malekos Smith, a senior associate at the Center for Strategic and International Studies, suggests developing defensive mechanisms using technology to aid information processing, pattern recognition, and attribution.[35] At the macro level, artificial intelligence and machine learning can help identify patterns in a saturated information environment. Malekos Smith observes that—as the saying goes—"A lie can travel around the world while the truth is still putting on its shoes."[36] This statement highlights a commonly known fact regarding disinformation and underscores the persistent challenge that decisionmakers face. This challenge, coupled with the sheer volume and speed at which we access information, exceeds most individuals' capability to synthesize and analyze large amounts of information and promptly make sense of it.

Conclusion

DOD must prioritize the risks posed by the current (dis)information environment and recognize that U.S. military personnel lack the education, skills, and awareness to counter it. In cognitive warfare, even subtle events can generate compounding mental effects. Consequently, cognitive warfare can degrade individuals' ability to think and make decisions that challenge their known values. DOD must also develop measures to protect the joint force from disinformation attempts that seek to sow doubt. Leaders should frame the problem and use or develop counterstrategies that build individual competency to actively recognize disinformation and fight against it.

Acknowledging cognitive warfare as a threat is vital to developing strategies to neutralize or counter cognitive attacks. However, leaders must execute tangible follow-up actions to prepare the joint force to fight now and in the future. Conceptualizing the human dimension as a critical vulnerability will enable the development of offensive and defensive actions to protect it. Taking actions to improve and optimize cognitive defense capabilities will posture the joint force's transition from wars of attrition to the coming wars of cognition.[37]

Conserving a strong narrative as a center of gravity for each military branch while ensuring the basic standard of resilience effectiveness can be achieved with proper education, awareness, and standard operating procedures. Such programs would require all military personnel to participate in cognitive skills development training in their initial, quarterly, and annual training and should become woven into professional military education curricula. Protecting civilians from these same attacks would also require a preventive approach. Alternatively, reactive approaches to combating cognitive warfare are much more complex and expensive and only marginally effective.

Developing a cognitive defense framework suitable for military personnel and beyond will strengthen the resilience of U.S. military personnel, directly and indirectly. Risks to the U.S. military population are not declining; these risks will only increase as an adversary's preferred tactic. Leaders must implement cognitive defense as a core DOD competency. **JFQ**

Notes

[1] Quoted in Elsa B. Kania, "Minds at War: China's Pursuit of Military Advantage Through Cognitive Science and Biotechnology," *PRISM* 8, no. 3 (2020), https://ndupress.ndu.edu/portals/68/documents/prism/prism_8-3/prism_8-3_kania_82-101.pdf.

[2] *François du Cluzel*, *Cognitive Warfare* (Norfolk, VA: NATO Allied Command Transformation, 2021), 6, https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf. Emphasis in original.

[3] Alexis Artwohl, "Perceptual and Memory Distortion During Officer-Involved Shootings," *FBI Law Enforcement Bulletin* 71, no. 10 (October 2002), 18, https://www.ojp.gov/ncjrs/virtual-library/abstracts/perceptual-and-memory-distortion-during-officer-involved-shootings; Dave Grossman, with Loren W. Christensen, *On Combat: The Psychology and Physiology of Deadly Conflict in War and in Peace*, 3rd ed. (Millstadt, IL: Warrior Science Publications, 2008), 31.

[4] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 80–81.

[5] Charles Cleveland et al., *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Amherst, NY: Cambria Press, 2018), 26.

[6] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004), 239.

[7] Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

[8] Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), 70–89, https://www.airuniversity.af.edu/portals/10/ssq/documents/volume-12_issue-3/ssqfall2018.pdf.

[9] Lennart Maschmeyer, "Digital Disinformation: Evidence from Ukraine," *Center for Security Studies Analyses in Security Policy* 278 (February 2021), 4, https://doi.org/10.3929/ethz-b-000463741.

[10] Erik C. Nisbet and Olga Kamenchuk, "The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy," *The Hague Journal of Diplomacy* 14, nos. 1–2 (April 2019), 65–82, https://brill.com/view/journals/hjd/14/1-2/article-p65_6.xml.

[11] Xie Kai [谢恺], Sun Hongwei [孙宏伟], and Li Wenqing [李文清], "Pay Attention to New Features of Strategic Deterrence" [关注战略威慑新特点], *PLA Daily*, November 30, 2021, quoted in Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, RRA853-1 (Santa Monica, CA: RAND, 2023), 39, 129, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA800/RRA853-1/RAND_RRA853-1.pdf.

[12] 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 (2020), 1–18, https://doi.org/10.1093/jogss/ogac016.

[13] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RR-1708-OSD (Santa Monica, CA: RAND, 2018), 86–89, https://www.rand.org/pubs/research_reports/RR1708.html.

[14] Engstrom, *Systems Confrontation and System Destruction Warfare*.

[15] Geoffrey Parker, ed., *The Cambridge History of Warfare* (New York: Cambridge University Press, 2005), 1–11; Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, *Understanding a New Era of Strategic Competition*, RRA290-4 (Santa Monica, CA: RAND, 2022), 6–7, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA290-4/RAND_RRA290-4.pdf.

[16] Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W.W. Norton and Company, 2011), 9.

[17] Mark Scott, "Russia and China Target U.S. Protests on Social Media," *Politico*, June 1, 2020, http://politico.eu/article/russia-china-us-protests-social-media-twitter/.

[18] Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 2020), IV-22.

[19] W. Eric Cobb, *Z-Health R-Phase Certification Manual*, 5th ed. (Tempe, AZ: Z-Health Performance Solutions, 2013), 5.

[20] Jordan B. Peterson, *12 Rules for Life: An Antidote to Chaos* (Toronto: Random House Canada, 2018), 87.

[21] Karen Glanz and Barbara K. Rimer, *Theory at a Glance: A Guide for Health Promotion Practice* (Bethesda, MD: National Cancer Institute, 1997).

[22] Jason M. Satterfield, *Mind-Body Medicine: The New Science of Optimal Health* (Chantilly, VA: The Teaching Company, 2013), 25.

[23] Satterfield, *Mind-Body Medicine*.

[24] Amy Mitchell et al., *Distinguishing Between Factual and Opinion Statements in the News* (Washington, DC: Pew Research Center, 2018), https://www.csus.edu/indiv/f/friedman/fa2019/govt1/schedule/a/fact-opinion.pdf.

[25] J. "Zhanna" Malekos Smith, "The Best Natural Defense to Psychological Warfare," *Small Wars Journal*, December 25, 2016, https://smallwarsjournal.com/jrnl/art/the-best-natural-defense-to-psychological-warfare.

[26] Smith, "The Best Natural Defense to Psychological Warfare."

[27] Nisbet and Kamenchuk, "The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy."

[28] Shannon L. Exley and Lindsay M. Oberman, "Repetitive Transcranial Magnetic Stimulation for the Treatment of Depression, Post-Traumatic Stress Disorder, and Suicidal Ideation in Military Populations: A Scholarly Review," *Military Medicine* 187, nos. 1–2 (January/February 2022), 73, https://doi.org/10.1093/milmed/usab187.

[29] Peter W. Singer and Eric B. Johnson, "The Need to Inoculate Military Servicemembers Against Information Threats: The Case for Digital Literacy Training for the Force," *War on the Rocks*, February 1, 2021, http://warontherocks.com/2021/02/we-need-to-inoculate-military-servicemembers-against-information-threats-the-case-for-digital-literacy-training/.

[30] "Cyber Florida, Florida Center for Instructional Technology, and New America Launch New Partnership to Improve 'Cyber Citizenship' Skills for K-12 Students," *New America*, December 16, 2020, https://www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship/.

[31] "Randomized Control Trial Finds IREX's Media Literacy Messages to Be Effective in Reducing Engagement With Disinformation," IREX, October 20, 2020, https://www.irex.org/news/randomized-control-trial-finds-irexs-media-literacy-messages-be-effective-reducing-engagement.

[32] Singer and Johnson, "The Need to Inoculate Military Servicemembers Against Information Threats."

[33] Linda Slapakova, "Towards an AI-Based Counter-Disinformation Framework," *The RAND Blog*, March 29, 2021, https://www.rand.org/blog/2021/03/towards-an-ai-based-counter-disinformation-framework.html.

[34] Slapakova, "Towards an AI-Based Counter-Disinformation Framework."

[35] Malekos Smith, "The Best Natural Defense to Psychological Warfare."

[36] Smith, "The Best Natural Defense to Psychological Warfare."

[37] Megan Friedl, "Goldfein Delivers Air Force Update," U.S. Air Force, September 19, 2017, https://www.af.mil/News/Article-Display/Article/1316603/goldfein-delivers-air-force-update/.