OCCASIONAL PAPER | NOVEMBER 2025

JSOU PRESS

COGNITIVE WARFARE TO DOMINATE AND REDEFINE ADVERSARY REALITIES: IMPLICATIONS FOR U.S. SPECIAL OPERATIONS FORCES

BY JEREMIAH "LUMPY" LUMBACA, PhD

On the cover:

The battlefield of the future is the human mind, and the very concepts of reality and truth are the target. Cognitive warfare goes far beyond traditional psychological operations; this new form of conflict combines cyber tools, psychological sciences, and neurosciences to alter perceptions and influence decision-making. Source: Image generated using Google Gemini 2.5 Flash, July 2, 2025.

JSOU Press
Melanie Casey, Editor in Chief
Beth DeGeorge, Editor
Alina Alvarez Perez, Editor
Design and layout by Arianna Czesler

Digital Version

JSOU Report 25-23
November 2025

Cognitive Warfare to Dominate and Redefine Adversary Realities: Implications for U.S. Special Operations Forces

BY JEREMIAH “LUMPY” LUMBACA, PhD

JSOU PRESS

Part 1: Cognitive Warfare Foundations

Consider the power to dictate who is perceived as "right" or "wrong" in conflicts like the Russia–Ukraine War or Israeli–Gazan conflict, or to reshape the outcome of a nation's election in the minds of its citizens. Imagine the U.S. and its allies not merely swaying opinions but reconstructing the very reality in which adversaries like North Korea, the Chinese Communist Party (CCP), Iran, or violent extremists make judgments, aligning their perceptions with U.S. strategic objectives.

In an era of strategic competition where gray zone conflict and hybrid warfare tactics are now commonplace, the human mind has emerged as a distinct and critical domain of conflict. There are differing definitions of the term cognitive warfare. Bernard Claverie and François du Cluzel define it as "an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, provoke thought distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels."[1] NATO's strategic warfare development command, known as Allied Command Transformation, notes that cognitive warfare includes "activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviors, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary."[2] Whole-of-society manipulation is a new norm.[3]

It is necessary to differentiate cognitive warfare from established concepts such as psychological operations (PSYOPS, sometimes referred to in defense circles as military information support operations [MISO]), information warfare, cyber warfare, and hybrid warfare.[4] Claverie and du Cluzel write:

> Cognitive [w]arfare is where all the elements of information warfare—including the operational aspects of psychology and neurosciences, based on systemics and complexity—combine for military action. It sits at the intersection of two operational fields that hitherto were managed separately: PSYOPS and influence operations (soft power) on the one hand, and cyber operations (cyber defence) intended to degrade or destroy physical information assets on the other. This intersection makes it possible to unite concepts and points of view from different scientific, military, or intelligence communities of interest, bringing about an interdisciplinary approach to how technologies impact humankind[5] (see Fig. 1).

In this sense, cognitive warfare may be thought of as a strategic discipline that directly targets the way individuals and groups think, perceive, process information, and ultimately act. Generating cognitive effects as the primary objective distinguishes it from mere information dissemination or information warfare.[6] See Figure 2 for a graphic representation of the conceptual

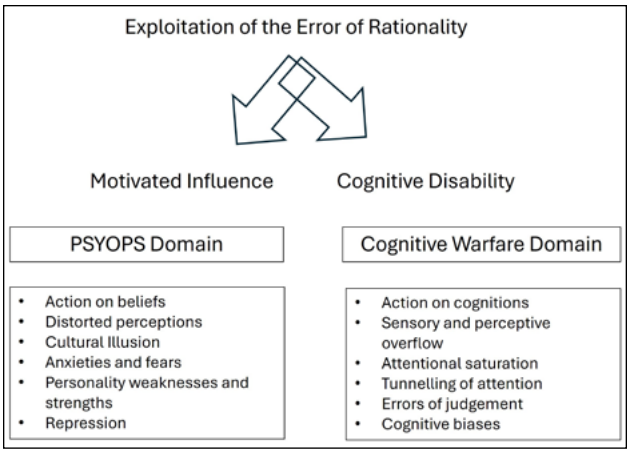

Figure 1. Differences between cognitive warfare and PSYOPS. Source: Author (data from Bernard Claverie and François du Cluzel, "The Cognitive Warfare Concept," NATO Innovation Hub for Allied Command Transformation, 2022.

relationships between these types of "warfare." As Alina Bârgăoanu and Flavia Durach explain, "this new type of warfare is waged by means of disinformation, propaganda, influence operations, and hostile information campaigns all at the same time. Above all, this new type of warfare is waged in a completely changed communication and information ecosystem, where every major issue in a society can be weaponized thanks to the very connectivity of that new ecosystem. Conceptualizing cognitive warfare as a new, technology-driven phenomenon has implications for research and for policymaking."[7]

Technological advancements are consistently highlighted as a key enabler and accelerant of cognitive warfare. The pervasive influence of social media and digital platforms is a recurring focus,[8] illustrating how these channels facilitate the rapid and mass dissemination of narratives, enabling precise manipulation of public opinion. Artificial intelligence (AI) is identified as a transformative force, with discussions revolving around its use for micro-targeting, generating hyper-realistic disinformation (e.g., deepfakes),[9] analyzing psychological profiles, and automating influence campaigns on an unprecedented scale. Furthermore, the increasing integration of insights from neuroscience[10] and behavioral science is seen as allowing for more precise and effective manipulation techniques, even leading to speculation about the theoretical implications of neuro-technologies and brain-computer interfaces.

Cognitive warfare is often presented as offering asymmetric advantages, allowing actors with fewer conventional military capabilities to undermine stronger adversaries by eroding their internal cohesion and decision-making processes.

Academic research dedicates considerable attention to cognitive warfare strategies employed by various state and non-state actors. Case studies, particularly those involving influence operations attributed to the CCP's cognitive warfare against Taiwan, are informative and provide empirical grounding for theoretical frameworks.[11] Cognitive warfare is often presented as offering asymmetric advantages, allowing actors with fewer conventional military capabilities to

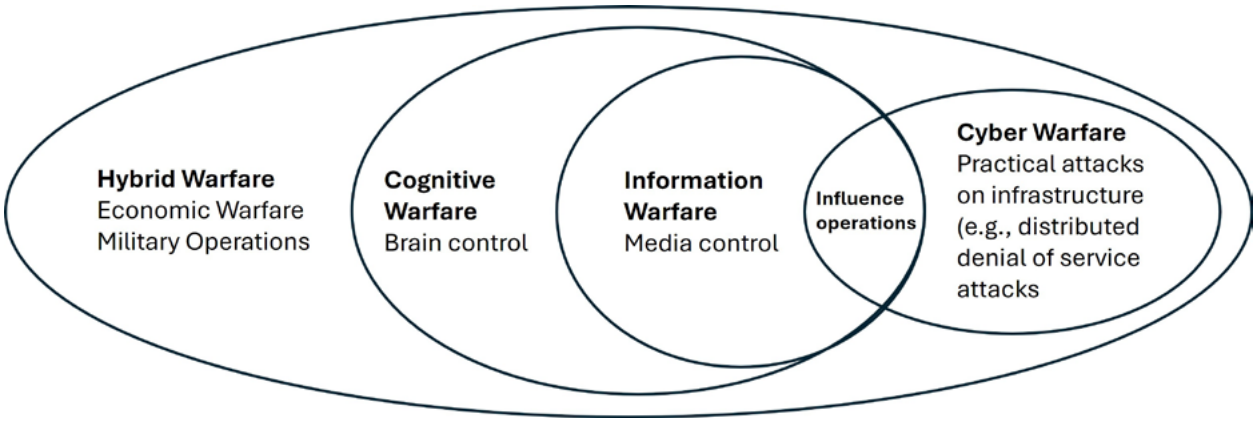

Figure 2. The conceptual relationship among cognitive warfare and other types of warfare. Source: Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," Journal of Global Security Studies 7, no. 4 (2022).

undermine stronger adversaries by eroding their internal cohesion and decision-making processes.

Part 2: Unleashing Cognitive Warfare

Creating and Defending Against Alternate Realities

Cognitive warfare penetrates the processes of perception, judgment, and belief formation. At its most sophisticated, this could involve the deployment of cognitive contagions—ideologically charged constructs that spread virally across digital and social networks influencing beliefs, emotional reactions, and ultimately behavior. The ultimate result of effective cognitive warfare may be that, after these operations take place over long periods of time using cognitive biases, they modify the thinking habits of the target. As Claverie and du Cluzel write, "They have lasting, even irreversible effects on the cognitive personality, i.e., the way in which an individual processes information."[12]

Unlike traditional disinformation campaigns, which rely on pushing falsehoods or misleading narratives, cognitive contagions embed particular patterns of thinking. These may include logical fallacies, emotionally-charged heuristics, and cognitive shortcuts that allow the contagions to self-propagate within communities. Rather than transmitting standalone messages, they act more like ideological malware, replicating and adapting to embed themselves in the mental frameworks of individuals and groups.[13] For example, emotionally resonant slogans, such as those that stoke fear or indignation, can bypass rational analysis and lodge deeply within a person's worldview. With repetition and social reinforcement, such beliefs can become difficult to dislodge, leading to what scholars describe as epistemic closure,[14] where new information is rejected if it contradicts the engineered narrative.

These contagions thrive in digital environments where information overload pushes users toward mental shortcuts[15] where echo chambers[16] reinforce existing

views and social media algorithms prioritize engagement over accuracy. Psychographic targeting, enabled by troves of user data, allows these cognitive viruses to be tailored with precision[17] to individual psychological profiles.[18] The result is a potent blend of personalization, repetition, and emotional provocation that erodes critical thinking and reshapes the architecture of public perception.

Drawing inspiration from quantum mechanics, one might consider a state of "narrative superposition" where multiple contradictory narratives exist simultaneously. The collapse of shared reality's "waveform" occurs, forcing the adoption of a dominant, desired reality. This parallels work in quantum cognition.[19] Manipulating perception itself can occur through virtual reality, augmented reality, or even targeted neuro-stimulation. While theoretical, these "sensory override" realities could directly influence an individual's experience and understanding of the world.[20]

Proactive measures include the widespread dissemination of advanced psychological inoculation and prebunking programs.[21] These efforts would likely leverage digital games and interactive simulations designed to build robust mental resistance[22] against cognitive contagions, moving beyond simple fact-checking. Concurrently, deep cognitive hygiene education[23] should be integrated into national curricula,[24] equipping citizens with the ability to deconstruct complex manipulation tactics, understand their own cognitive biases, and critically evaluate the emotional and logical underpinnings of information. To address vulnerabilities, efforts must focus on algorithmic recalibration[25] and counter-amplification,[26] advocating for and developing technologies that incentivize social media platforms to prioritize accuracy and diverse viewpoints over sensationalism. This could involve "white-hat"[27] algorithmic interventions that subtly disrupt the virality of harmful cognitive contagions. Finally, advanced inauthentic actor detection and disruption require public–private partnerships, leveraging AI and machine learning to identify and neutralize botnets, synthetic media, and coordinated inauthentic behavior. This would also involve the deployment of "cognitive antibodies," automated systems that intelligently detect and flag manipulated content or suspicious narrative patterns in real time.[28]

Strategic manipulation may not necessarily target societies broadly or groups generically, but rather individuals specifically.[29] This form of warfare would rely on constructing detailed psychographic profiles drawn from exhaustive data, online behaviors, biometric indicators, purchase histories, sleep patterns, even vocal tonality.[30] These profiles would then be used to tailor ideological messaging in ways that bypass conscious resistance, tapping into subconscious vulnerabilities, emotional needs, and cognitive biases. See Figure 3.

Counter-Cognitive Strategies

As cognitive warfare strategies evolve to target the perceptual and psychological integrity of individuals, new modes of defense must emerge. Beyond training modules, simulations may offer even greater potential. These controlled manipulation

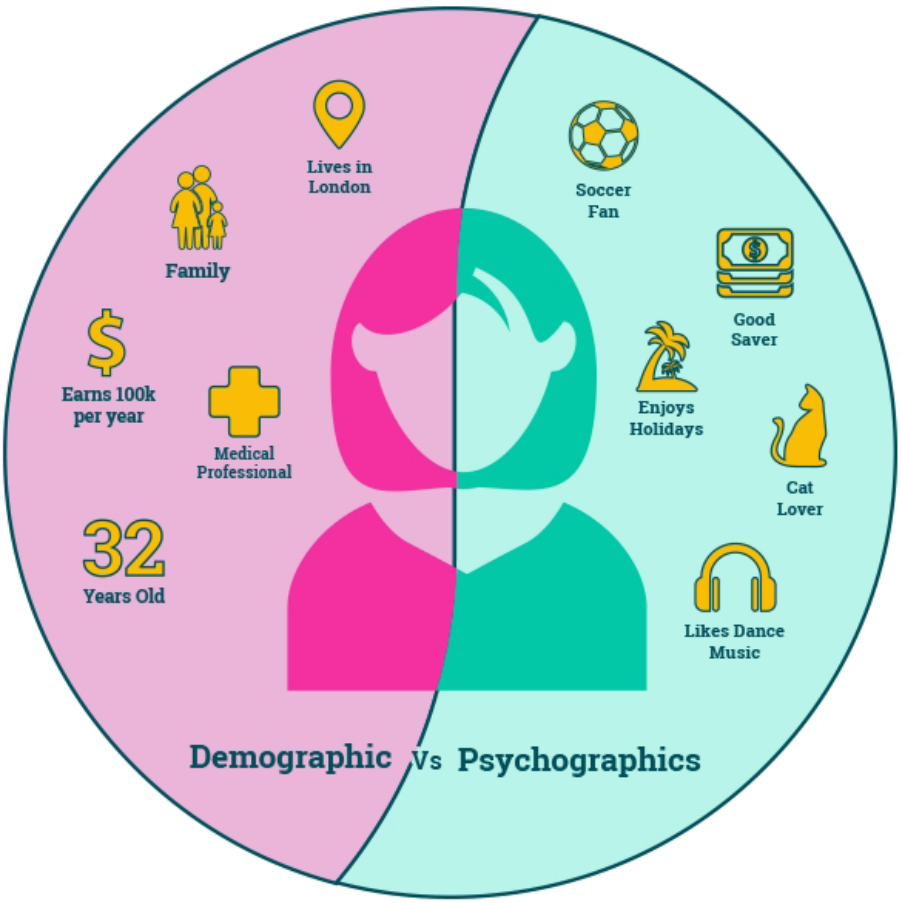

Figure 3. This graphic illustrates the difference between demographics and psychographics using a stylized profile of an individual showing what can be defined as demographic data—quantifiable information like age, location, occupation, etc.—and what can be defined as psychographic data, such as an individual's interests, lifestyle, and personality traits. Source: CBInsights.

environments could place users in scenarios where they experience synthetic influence campaigns firsthand while being guided by educational feedback. Just like military wargames build tactical proficiency, these cognitive simulations would train individuals to recognize psychological operations in real time and critically assess their own responses. Research in the field of serious games[31] and experiential learning[32] indicates that such methods enhance critical thinking, emotional regulation, and pattern recognition under stress.

Rather than simply automating detection of disinformation, AI can be used to construct cognitive firewalls that identify manipulative content patterns and intervene with user-centered prompts that encourage reflection. For example, if a user is exposed to emotionally manipulative headlines or ideologically extreme narratives, the system might surface prompts like, "Would you like to see how others view this issue?" or "Here

is a contrasting viewpoint based on verified sources." Research by Brundage et al. highlights the importance of aligning AI with societal values and proposes mechanisms by which AI systems can support human autonomy while countering information-based threats.[33]

Just as cybersecurity evolved from protecting physical servers to protecting identities, cognitive security must evolve from guarding against lies to preserving the mental sovereignty of individuals. This new era of defense will require collaboration between psychologists, AI developers, educators, ethicists, and strategic planners.

Such firewalls would leverage computing and sentiment analysis to determine the emotional charge of digital content, identify polarizing or deceptive cues, and deliver subtle interventions before belief entrenchment occurs. These mechanisms could be embedded in browsers, content platforms, and educational tools—much like spell-checkers or ad blockers, but for cognitive hygiene. Experimental prototypes in this domain already exist, such as "crankiness detectors" for news headlines and predictive models of ideological extremism based on digital activity.[34]

These counter-cognitive systems must be designed carefully. Overly paternalistic or coercive interventions could backfire, reinforcing paranoia or perceptions of censorship. As philosopher Onora O'Neill emphasizes in discussions on trust and communication, credibility must be earned through transparency, not enforced by fiat.[35] Therefore, explainability, open-source design, and opt-in protocols should ideally guide the development of cognitive defense systems.[36] Just as cybersecurity evolved from protecting physical servers to protecting identities, cognitive security must evolve from guarding against lies to preserving the mental sovereignty of individuals. This new era of defense will require collaboration between psychologists, AI developers, educators, ethicists, and strategic planners.

Proactive strategies could include the strategic erosion of adversary cognitive resilience, actively identifying and exploiting weaknesses in their defense mechanisms. This could involve saturating their information environment with rapidly evolving and novel forms of influence that overwhelm their detection systems or introducing subtle, continuous cognitive stressors designed to erode a target population's capacity for critical thinking over time. A more audacious approach would involve the gradual introduction of narratives and "cognitive anchors" that predispose target audiences to interpretations of events favorable to U.S. interests, even before critical events unfold. The goal here is to proactively shape their perceptual framework.

Furthermore, the development and deployment of AI-driven bots for narrative

dominance would disrupt adversary influence operations by introducing noise, doubt, or alternative framings. Finally, while maintaining adherence to international law, it is worth exploring how AI can be used for algorithmic truth distortion for adversary narratives. This might involve applying AI to identify logical inconsistencies, internal contradictions, or emotional manipulation within adversary propaganda and then using subtle, algorithmically driven interventions to highlight these flaws to their own populations.

Cognitive Geopolitics

As information flows, identity narratives and cognitive infrastructures become strategic assets, and a new domain of geopolitical contestation emerges. The ability to shape global perceptions increasingly translates into tangible geopolitical advantage. States that dominate the information ecosystem can influence elections, shape diplomatic discourse, and frame conflicts in ways that legitimize their actions while delegitimizing their adversaries. Control over cognitive infrastructure—such as search engines, news aggregators, and social media platforms—becomes a tool for soft power and, at times, hybrid warfare. This is particularly evident in global information campaigns conducted by state actors where disinformation is not simply about spreading falsehoods but about undermining shared truth and eroding democratic consensus.

These dynamics raise the specter of a "cognitive arms race," where states begin to invest heavily in both offensive and defensive cognitive capabilities. Just as nuclear and cyber weapons prompted the development of deterrence doctrines and red lines, so too might we see the emergence of doctrines around cognitive sovereignty, disinformation deterrence, and psychological countermeasures.[37] In this scenario, state and non-state actors engage in escalating contests to manipulate, protect, or destabilize the mental frameworks of target populations, both foreign and domestic.

In response, cognitive deterrence strategies may be necessary. This implies the need for doctrines that define thresholds for retaliatory action when adversaries engage in manipulative perception-shaping. This might include identifying unacceptable interference in democratic discourse or national identity formation. The challenge lies in attribution: cognitive warfare rarely leaves fingerprints. Influence campaigns are diffused, plausibly deniable, and deeply entangled with civilian platforms and behaviors. As AI and neurotechnology advance, it is reasonable to assume that the tools available for manipulating perception will become increasingly powerful. The

The Dormio device is a wearable system developed by scientists at MIT to interact with dreams. It is worn on the hand and uses sensors to track a user's physiological signs to detect the onset of sleep then deliver targeted audio cues to influence the content of dreams in the hypnagogic state.
Photo by Oscar Rosello

ability to simulate convincing yet deceptive realities will increase exponentially.

Proactive epistemic sovereignty safeguards are crucial and involve the implementation of national policies and investment in domestic epistemic infrastructures, such as public broadcasters and independent research institutions. Simultaneously, international norm development for cognitive security will become increasingly necessary, aiming to establish clear norms, agreements, and "red lines" for acceptable and unacceptable cognitive influence operations, including developing shared attribution mechanisms for malign activities.

Aggressive narrative dominance and framing will be needed to establish and maintain control over key geopolitical issues, proactively framing conflicts and events in ways that legitimize U.S. actions and delegitimize adversary behavior on the global stage.

The development of AI-driven early warning and threat assessment systems capable of real-time, global monitoring of cognitive warfare campaigns, identifying emergent threats, attributing sources where possible, and providing rapid threat assessment, is vital. Strategic communications for resilience-building involve not only countering adversary narratives but also proactively informing domestic and allied populations about the nature of cognitive warfare—building collective awareness and resilience against manipulation.

A more aggressive strategy includes implementing cognitive colonialism/imperialism reversal in regions where adversarial worldviews have been imposed.[38] This means the use of carefully crafted, culturally resonant information campaigns that promote alternative perspectives, empower local epistemologies, and subtly challenge the foundational assumptions of adversary-imposed realities. Concurrently, aggressive narrative dominance and framing will be needed to establish and maintain control over key geopolitical issues, proactively framing conflicts and events in ways that legitimize U.S. actions and delegitimize adversary behavior on the global stage.

The formulation and open articulation of a cognitive deterrence doctrine would clearly outline thresholds for retaliatory cognitive actions when adversaries engage in unacceptable perception-shaping operations against U.S. interests or allies, signaling a willingness to engage forcefully in the cognitive domain. Finally, within legal frameworks, there is potential for the exploitation of adversary cognitive infrastructures. This will involve identifying and leveraging vulnerabilities within their systems, such as search engines and social media platforms, to subtly introduce information that undermines their internal cohesion, challenges their state narratives, or promotes dissent that serves U.S. strategic

interests through open-source intelligence and public engagement tactics.

Part 3: Implications for U.S. Special Operations Forces

U.S. Special Operations Forces (SOF) are currently not trained, organized, or equipped for a future dominated by cognitive warfare. While U.S. Special Operations Command (USSOCOM), theater special operations commands (TSOCs), and their subordinate units have command surgeons focused on physical health, for example, they lack neuroscientists, behavioral scientists, cognitive psychologists, or cognitive engineers who could help understand, shape, project, and defend against operations aimed at the human mind.[39]

Operational teams deploy with state-of-the-art satellite communications equipment to relay battlefield information across continents, yet they do not possess the equivalent "cognitive toolkits," such as advanced brain-computer interfaces, intelligent psychological monitoring systems like smart sensor bracelets that track emotional states in real time, or tools to disrupt adversarial narratives.[40] This personal erosion of objectivity mirrors broader vulnerabilities, where cognitive warfare exploits human biases—such as the U.S.'s "WEIRD" (Western, educated, industrialized, rich, democratic)[41] psychological profile—to sow doubt and division, leaving forces like SOF ill-prepared to counter such threats. A small SOF team deployed overseas might find itself unknowingly outmaneuvered by malign narratives, deepfake videos portraying U.S. troops committing atrocities, viral rumors discrediting local leaders aligned with the U.S., or psychological campaigns designed to fracture trust within allied forces.

For example, in Africa, Chinese cognitive warfare campaigns have outpaced U.S. efforts, as noted by General Michael E. Langley, former Commander of U.S. Africa Command, who warned that Beijing's information manipulation is subordinating African nations' interests to China's, securing critical resources like rare earth minerals while eroding support for SOF missions in the region.[42] Similarly, Iranian botnets[43] have amplified anti-U.S. narratives, framing American actions as reckless and linking them to civilian casualties in the region, which complicates SOF coordination with Gulf allies and undermines regional stability. Russia's operations in Ukraine provide another anecdote using fake news and social media to blame others for atrocities, decaying public trust in open societies and forcing allies and partners to divert resources to counternarratives rather than kinetic operations.[44] The result is loss of military access, economic opportunities, and partnerships, with SOF often operating in environments where perceptions are pre-shaped against them.

To bridge this divide, SOF must evolve. USSOCOM Commander General Bryan P. Fenton emphasized the need to counter China and Russia in the information domain through (1) improved coordination and leadership in information operations across the Department of Defense and other government agencies; (2) increased investment in information operations to match the scale and sophistication of adversaries' efforts; and (3) empowering

lower-level commanders with the authority to conduct timely and effective information operations.[45]

> **U.S. SOF are positioned better than conventional forces to adjust course and eventually employ effective offensive and defensive cognitive warfare capabilities. SOF's specialized mission sets, cultural adaptability, and small-team autonomy provide a natural advantage in a domain where agility, precision, and influence matter.**

Despite these concerns, U.S. SOF are positioned better than conventional forces to adjust course and eventually employ effective offensive and defensive cognitive warfare capabilities. SOF's specialized mission sets, cultural adaptability, and small-team autonomy provide a natural advantage in a domain where agility, precision, and influence matter. Existing strengths in PSYOPS, civil affairs (CA), and unconventional warfare (UW) provide a solid foundation to build new capabilities on.

Defensive and offensive considerations for SOF in the cognitive warfare space are outlined below, but a key point must be made before proceeding. The ideas presented here for SOF are not intended to replace or alter the unique cultures and mission sets that exist throughout the special operations community. For example, Green Berets will continue to be the masters of UW and Navy SEALs will continue to be the go-to direct action force in the maritime domain. With that in mind, the following recommendations are intended to outline considerations for new tools, training, capabilities, and organization that enable those SOF communities to do their jobs more effectively in the near future.

Recommendations

To defend against malign cognitive warfare, SOF must first secure its own personnel and operations from manipulation. This goes beyond traditional operational security to include cognitive resilience. "Cognitive immunotherapy" programs can build a high level of epistemic self-awareness, enabling operators to recognize and resist manipulative tactics in real-time, even when these tactics are designed to exploit personal biases and values. As for equipping, SOF will require tools for monitoring and analysis. This includes AI-powered platforms that can detect subtle changes in local information environments, identify inauthentic actors, and flag potential cognitive contagions. At some point, personal equipment will need to include integrated cognitive firewalls, systems that provide real-time alerts about the emotional and logical underpinnings of information being consumed. These will help preserve clear-headed assessments in a chaotic information space.

Regarding SOF organization, some type of "cognitive warfare cells" should be stood up at all echelons, from TSOCs down to

operational detachments. These cells would be multi-disciplinary, including not only PSYOP and CA specialists, but also data scientists, behavioral psychologists, and AI experts. Their primary mission would be to analyze adversarial cognitive operations and develop tailored defensive strategies for SOF and partner forces.

While defending against cognitive threats is crucial, SOF's higher payoff likely lies in its ability to conduct offensive cognitive warfare. This means using AI tools to create psychographic profiles of target groups and individuals within an adversary's ranks or populace. Operators must learn to craft and deploy micro-narratives that exploit cognitive biases and create narrative superposition, a state of doubt that ultimately forces the adoption of U.S.-aligned perspectives.

These tools will allow operators to adapt messaging based on real-time feedback from the target audience's information environment. SOF has the ability in this case to subtly shape a target area or an individual's information environment by exploiting vulnerabilities to amplify pro-U.S. narratives.

Conclusion

Cognitive warfare has the potential to redefine not only adversarial realities but also the operational effectiveness of U.S. SOF. Concepts ranging from cognitive contagions and personalized influence to counter-cognitive defenses and SOF-specific offensive applications underscore a reality: The battlefield of the future is increasingly mental. By integrating cognitive warfare into SOF's training, equipping, and organizational frameworks, the U.S. can leverage the unique capabilities of special operators to defend against malign influence and offensively shape adversary perceptions, ensuring strategic dominance in the cognitive domain. Admittedly, the human mind remains a "black box;"[46] and many ideas presented here are speculative, rooted in the logical extrapolation of current technological and cognitive trends. Some of these ideas admittedly seem far-fetched, the things of science fiction. With that thinking, one option might be to dismiss the concepts outlined above. By not exploring possibilities now, however, we ensure that America and its partners remain steps behind malign actors that are already experimenting in this space. For these reasons, America should instead take the possibilities in cognitive warfare seriously, and experiment now. Resilience in defense and creativity in cognitive warfare offense may well define the future relevance and dominance of America, including its most agile military assets.

Notes

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

2. "Cognitive Warfare," NATO Allied Command Transformation, accessed July 3, 2025, https://www.act.nato.int/activities/cognitive-warfare/.

3. Robin Burda, "Cognitive Warfare as Part of Society: Never-Ending Battle for Minds" in *Paper Series: Information-Based Behavioural Influencing and Western Practice,* eds. Arthur Laudrain, Laura Jasper, and Michel Rademaker (The Hague Centre for Strategic Studies, 2023), https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf.

4. Johns Hopkins University and Imperial College London, "Countering Cognitive Warfare: Awareness and Resilience," *NATO Review*, May 20, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

5. Claverie and du Cluzel, "The Cognitive Warfare Concept."

6. Martin C. Libicki, *What Is Information Warfare?* (National Defense University, 1995), https://apps.dtic.mil/sti/citations/ADA367662.

7. Alina Bârgăoanu and Flavia Durach, "Cognitive Warfare: Understanding the Threat," in *Routledge Handbook of Disinformation and National Security*, eds. Rubén Arcos, Irene Chiru, and Cristina Ivan (Routledge, 2023): 221–236, https://doi.org/10.4324/9781003190363.

8. Sarah Bradshaw and Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns," *Journal of International Affairs* 71, no. 1.5 (2018): 23–32.

9. Hany Farid, "Creating, Using, Misusing, and Detecting Deep Fakes," *Journal of Online Trust and Safety* 1, no. 4 (2022): 1–33, https://doi.org/10.54501/jots.v1i4.56.

10. James Giordano, ed., *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Press, 2014), https://doi.org/10.1201/b17454.

11. Ying-Yu Lin, "China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures," *Taiwan Strategists*, no. 20, 37–54, https://www.airitilibrary.com/Article/Detail?DocID=P20220613001-N202312210022-00003; Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2713.html.

12. Claverie and du Cluzel, "The Cognitive Warfare Concept."

13. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Eamon Dolan/Houghton Mifflin Harcourt, 2018); Anton Kühberger "The Framing of Decisions: A New Look at Old Problems," *Organizational Behavior and Human Decision Processes* 62, no. 2 (1995): 230–240, https://doi.org/10.1006/obhd.1995.1046.

14. Cass R. Sunstein, *On Rumors: How Falsehoods Spread, Why We Believe Them, and What Can Be Done* (Princeton University Press, 2014).

15. Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011).

16. Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin Press, 2011).

17. Muhammed Haroon et al., "YouTube, The Great Radicalizer? Auditing and Mitigating Ideological Biases in YouTube Recommendations," March 20, 2022, https://doi.org/10.48550/arXiv.2203.10666.

18. *The Great Hack*, directed by Karim Amer and Jehane Noujaim (2019, Noujaim Films and The Othrs), Netflix.

19. Jerome R. Busemeyer and Peter D. Bruza, *Quantum Models of Cognition and Decision* (Cambridge University Press, 2012), https://doi.org/10.1017/CBO9780511997716.

20. Michael Madary and Thomas K. Metzinger, "Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology," *Front. Robot. AI*, no. 3 (2016): 1–23.

21. Laura Garcia and Tommy Shane, "A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation," *First Draft News*, last reviewed June 29, 2021, archived August 25, 2025, at https://web.archive.org/web/20240715231600/https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/#expand.

22. William J. McGuire, "Some Contemporary Approaches," *Advances in Experimental Social Psychology* 1 (1964): 191–229, https://doi.org/10.1016/S0065-2601(08)60052-0.

23. Eliza Mackintosh and Edward Kiernan, "Finland Is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy," *CNN*, May 2015, https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

24. "Media Literacy and Education in Finland," *Finland Toolbox*, March 12, 2024, https://toolbox.finland.fi/life-society/media-literacy-and-education-in-finland/.

25. Benjamin Laufer and Helen Nissenbaum, "Algorithmic Displacement of Social Trust," in *Optimizing for What? Algorithmic Amplification and Society* (Knight First Amendment Institute at Columbia University, 2023), https://ssrn.com/abstract=4734544.

26. Ferenc Huszár et al., "Algorithmic Amplification of Politics on Twitter," *Proceedings of the National Academy of Sciences* 119, no. 1 (2021), https://doi.org/10.1073/pnas.2025334119.

27. Tyrone C. Gubler, "The White-Hat Bot: A Novel Botnet Defense Strategy" (master's thesis, Air Force Institute of Technology, 2012), https://scholar.afit.edu/etd/1113.

28. AIT Staff Writer, "Adversarial Machine Learning in Detecting Inauthentic Behavior on Social Platforms," *AIThority*, May 7, 2025, https://aithority.com/machine-learning/adversarial-machine-learning-in-detecting-inauthentic-behavior-on-social-platforms/.

29. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

30. Michal Kosinski et al., "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences* 110, no. 15 (2013), https://doi.org/10.1073/pnas.1218772110.

31. James Paul Gee, "What Video Games Have to Teach Us About Learning and Literacy," *Computers in Entertainment* 1, no. 1 (2003): 20, https://doi.org/10.1145/950566.950595.

32. Chris Dede, "Immersive Interfaces for Engagement and Learning," *Science* 323, no. 5910 (2009): 66–69, https://doi.org/10.1126/science.1167311.

33. Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *Scholarly Works – Centre for Research in the Arts, Social Sciences and Humanities* (Apollo - University of Cambridge Repository, 2018), https://doi.org/10.17863/CAM.22520.

34. Manoel Horta Ribeiro et al., "Auditing Radicalization Pathways on YouTube," paper presented at the Conference on Fairness, Accountability, and Transparency, January 2020, 131–141, https://doi.org/10.1145/3351095.3372879.

35. Onora O'Neill, host, *The Reith Lectures: A Question of Trust*, BBC, 2002, https://www.bbc.co.uk/programmes/p00ghvd8/episodes/player.

36. Jane R. Garrison et al., "Monitoring What Is Real: The Effects of Modality and Action on Accuracy and Type of Reality Monitoring Error," *Cortex; A Journal Devoted to the Study of the Nervous System and Behavior* 87 (2017): 108–117, https://doi.org/10.1016/j.cortex.2016.06.018.

37. Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017), https://doi.org/10.2307/j.ctt1trkjd1.

38. Marie Battiste, "Cognitive Imperialism," in *Encyclopedia of Educational Philosophy and Theory*, ed. Michael A. Peters (Springer Singapore, 2017), 183–188, https://doi.org/10.1007/978-981-287-588-4_501.

39. Andrew MacDonald and Ryan Ratcliffe, "Cognitive Warfare: Maneuvering in the Human Dimension," *Proceedings* 149, no. 4 (2023): 1,442, https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension.

40. Josh Baughman and Peter W. Singer, "China Gears Up for Cognitive Warfare," *Defense One*, April 7, 2023, https://www.defenseone.com/ideas/2023/04/china-gears-cognitive-warfare/384876/; Brian Godwin, "From Perception to Protection: Countering Cognitive Warfare in the U.S. Army" (master's thesis, U.S. Army Command and General Staff College, 2023), https://cgsc.contentdm.oclc.org/digital/api/collection/p4013coll2/id/4112/download.

41. Joseph Henrich, *The Weirdest People in the World: How the West Became Psychologically Peculiar and Particularly Prosperous* (Farrar, Straus and Giroux, 2020).

42. *Statement Before the United States Senate Committee on Armed Services* (2024) (statement of Commander General Michael E. Langley, U.S. Africa Command).

43. Babak Taghvaee, "Iran's Use of Psychological Warfare Against Its Adversaries and Strategies for Deterrence," *Middle East Quarterly* 32, no. 3 (2025), https://www.meforum.org/meq/irans-use-of-psychological-warfare-against-its-adversaries-and-strategies-for-deterrence.

44. Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media* (RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RR4373z2.html.

45. Austin Branch et al., "America Is Being Out-Gunned in Cognitive Warfare," *Information Professionals Association*, June 23, 2025, https://information-professionals.org/america-is-being-out-gunned-in-cognitive-warfare/.

46. "Prying Open the Black Box of the Brain," *U.S. National Science Foundation*, June 12, 2013, https://www.nsf.gov/news/prying-open-black-box-brain.

About the Author

Jeremiah Lumbaca, PhD

Jeremiah "Lumpy" Lumbaca, PhD, is a retired U.S. Army Green Beret and current professor of irregular warfare, counterterrorism, and special operations with the Department of Defense. He can be found on X/Twitter @LumpyAsia.

The Joint Special Operations University (JSOU) Press is the scholarly publishing arm of U.S. Special Operations Command (USSOCOM). Through unclassified, open-access materials and SOF-relevant thought leadership, the press supports both the university and USSOCOM in advancing the SOF warrior mind. SOF-specific publications and research, enterprise-wide engagement, and an annual Academic Call for Special Operations Papers facilitate creative, innovative solutions in alignment with command priorities.

JSOU provides relevant joint special operations-peculiar education programs that strengthen the SOF enterprise's impact on the joint force and the Nation.

Joint Special Operations University
7701 Tampa Point Blvd.
MacDill AFB, FL 33621
jsou.edu/press

JSOU PRESS