Assessing â??Cognitive Warfareâ?•

Description

Editorâ??s Note: this article is being republished with the permission of Small Wars Journal as part of a republishing arrangement between IWI and SWJ. The original article was published on 11.14.2025 and is available here.

image

Despite its introduction over a decade ago by the Peopleâ??s Liberation Army, there is no common understanding of Cognitive Warfare. Nor is there an agreement on the existence of a human or cognitive domain. These concepts compete in a crowded and confusing field centered around information technology and the related information dimension of statecraft. While the US intelligence community notes the increasing prevalence of Chinese concepts and research for what they term Cognitive Domain Operations (as well as active Russian activities), there is little appreciation for the implications of Cognitive Warfare in the US military as described by the pacing threat.

Scholars have generated numerous labels to capture the ongoing evolution of information technologies as a vector to influence decision-makers and impact public opinion. See Figure 1 for a partial list. Recently, US government agencies have been using Foreign Malign Influence or just Influence Operations to address the threat.[1] RAND has published studies on cyber-enabled Influence Operations, Virtual Societal Warfare, and Next Generation Psychological Warfare to capture the contest in the information environment.[2] Related studies on Russian disinformation are also common, and with overlapping definitions.

War in the future will not be â??wars of attrition but wars of cognition.â?•

Now the concept of Cognitive Warfare is competing in this crowded space, with no accepted definition or understanding of how it fits within the national security agenda. While information and narratives have shaped wars in the past, ongoing technological developments provide extremely efficient tools to expand this battlespace and substantially raise the potential and salience of Cognitive Warfare. New communication tools now offer infinite possibilities for digital distortion, opening the way to achieving desired objectives in opponentsâ?? minds. Key competitors from autocratic states are not content to

merely control their own population; instead, they have â??weaponizedâ?• social media with â??algorithmic amplificationâ?• against Western societies.[3] In the words of one expert, war in the future will not be â??wars of attrition but wars of cognition.â?•[4] The joint warfighting community is aware of the challenge, but the national security community is reducing its ability to monitor and respond effectively.

Figure 1. Information Warfare Variants

To the historically oriented, the fight for the minds of decision-makers and noncombatants does not expand the battlespace, but it does expand or at least challenge long-held Western conceptions about war.[5] Those encultured with violent visions, per Clausewitz, will struggle with this concept. The acolytes of the Prussian sage think in terms of physical violence as the essence of war and overlook his description of war as a clash of wills, as well as his discussions about rational and irrational factors in human conflict.

Thus, Cognitive Warfare runs against the grain for the selective Clausewitzian reader, as it goes after a much softer target: the human mind. Because of this bias, Cognitive Warfare faces a steep uphill fight for acceptance within the US military establishment. The American predisposition to kinetic operations and attrition stems from the defense establishmentâ??s strategic culture. This stress on hard power is part of the prevailing conventional US strategic and military culture, which privileges strike operations in the physical realm over more unconventional approaches and especially those involving the human domain.[6] As Colin Gray noted long ago, the US military culture is thoroughly conventional, firepower-centric, and technologically oriented.[7]

This assessment reviews the literature and ongoing dialogue on Cognitive Warfare within the research community. The reviewed scholarship details relevant material from the Peopleâ??s Liberation Army (PLA), as well as from other international sources. The paper then moves to coverage on the subject in the United States. This analysis concludes with a brief assessment to further develop this framework.

Defining Cognitive Warfare

In Cognitive Warfare, the message is the munition, and the target is the mind of either specific individuals (e.g., elites, influencers, policymakers) or the collective population of a democratic state.

Distorting what these individuals think is a precursor to how they think, and thus how they behave.

Early advocates such as the French officer, Francois du Cluzel, defined Cognitive Warfare as â??the art of using technologies to alter the cognition of human targets, most often without their knowledge and consent.â?•[8] This early conception stressed Cognitive Warfare as an offensive form of cyber conflict; however, he recognized that countermeasures and preventive measures were required. Du Cluzel differentiated psychological operations from cognitive operations, but it is unclear whether the distinction is valid or of value. For du Cluzel, psychological warfare attempts to change what the target audience thinks, but Cognitive Warfare aims at shaping how they reason and their resultant behavior. This distinction lies at the heart of why human cognition is the central objective.

> Cognitive War is the application *of targeted and tailored messages and nonviolent methods used against civilian and military decision-makers or the general population of a target state to gain a positional advantage in the cognitive domain or gain desired political, military, and informational outcomes.*

While Cognitive Warfare is not new, there are a number of novel technologies that significantly enhance the reach and efficacy of activities that target the way decision-makers and individuals think about a crisis situation. Some have seen this as social media-based influence operations.[9] These technologies can be combined to â??assess, access, and affect the cognitive space.â?•[10] While our competitors think in terms of systems and confronting and deceiving us, Western militaries orient on hardware, maneuver platforms, and kinetic operations.

Cognitive Warfare but can be refined to capture a clear theory of victory focused on tailored actions in the information domain. My starting definition of Cognitive War is the application *of targeted and tailored messages and nonviolent methods used against civilian and military decision-makers or the general population of a target state to gain a positional advantage in the cognitive domain or gain desired political, military, and informational outcomes.* This definition aligns with most Western theorists, who focus on social media manipulation of civilian populations. There are limitations with this approach, which are addressed later.

State of the Security Literature

International Perspectives

There are numerous research articles throughout the international security community on this topic. NATO has continued to build upon Du Cluzelâ??s work.[11] Du Cluzel also recognized the array of new technologies that would increase the salience of Cognitive Warfare, including the weaponization of neuroscience and the potential convergence of nanotechnology, biotechnology, gene editing, computer science, information technologies, and cognitive sciences. His most recent work defined Cognitive Warfare as â??an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder action, with negative effects, both at the individual and collective level.â?• [12]

In the last two years, there has been a surge in interest in this mode of conflict in Europe and Asia.[13] Japanese military officers have tracked PLA developments closely and analyzed Russian efforts in Ukraine to assess how effective the information activity has been.[14] They assess the PLAâ??s interest in what they call â??Cognitive Domain Operationsâ?• (discussed in depth later) as strong and growing. Military analysts in India have also assessed PLA writings on the topic.[15]

Taiwan has studied and faced this threat. Their scholars erroneously think that cognitive warfare is part of the Chinese Communist Partyâ??s (CCP) strategy of â??unrestricted warfareâ?• (è¶ é?•æ?°). However, Taiwanese strategists correctly recognize that Cognitive Warfare targets human perception, attitudes, and decision-making through information manipulation, propaganda, and psychological operations with the intent of gaining strategic objectives. The Taiwanese Ministry of National Defense (MND) describes it as an effort â??to sway the subjectâ??s will and change its mindset. Psychologically, the PRC is trying to cause mental disarray and confusion, in order to weaken fighting will and determination to defending ourselves.â?•[16] The MND also assesses that cognitive warfare â??originated from the [disciplines] of intelligence warfare, psychological warfare, and public opinion warfare.â?• As a clear target in Chinaâ??s crosshairs, the government in Taiwan has set up a research center tasked with deflecting the PRCâ??s narratives.[17] This research concluded that the PRC has not been very effective despite continued pressure campaigns against Taipei.[18]

China and Cognitive Domain Operations

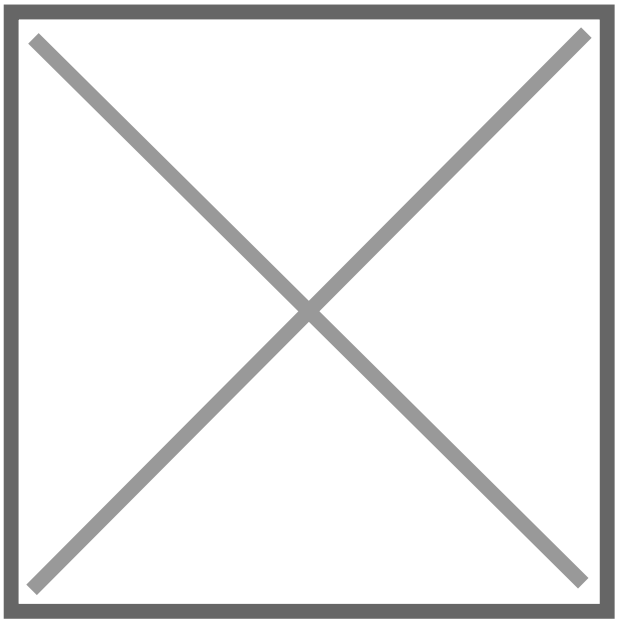
In contrast with US strategic and military culture, China has embraced the existence of a cognitive domain and has expanded its thinking about contemporary warfare. It views the cognitive space as increasingly central to future conflict. â??The cognitive domain will become another battle domain next to the land, sea, air, space, electromagnetic, and cyber domains of warfare.â?•[19] The PLA has been discussing the relevance of psychological conflict for several generations, but began writing about the cognitive domain as far back as 2002, with a steep increase in 2014. Some of these early Chinese

writers stressed the novelty of the cognitive space as â??a brand-new battlefield.â?•[20] [21]

Back in 2017, Major General He Fuchu forecasted, â??The sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness (æ?•è¯?å??); the human brain will become a new combat space.â?•[22] Consequently, success on the future battlefield will require achieving not only â??biological dominanceâ?• (å?¶ç??æ•?) but also â??mental/cognitive dominanceâ?• (å?¶è??æ•?) and â??intelligence dominanceâ?• (å?¶æ?ºæ•?).

Chinese analysts employ a deep historical perspective about the impact of technology over time, and they note that each industrial revolution has extended the reach and impact of information. Our current era, the Fourth Industrial Revolution, is said to extend the multimedia of the previous period with AI and image processing technologies to create deepfakes that can be used by the military to fool the enemy. â??Throughout the continuous evolution of technology, more and more media can be used,â?• one Chinese author notes, â??to influence the enemyâ??s thinking, judgment, and cognition, thus creating new modes of cognitive domain combat.â?•[23]

Chinese analysts have studied this aspect of modern conflict, and the government has supported research on how to translate the concept into an advantage for the PLA. This comports with the famous Sun Tzu maxim that equates winning without fighting as the highest form of the art of warfare.



Many scholars think this remains a key feature of Chinese strategic culture. Evidence for thinking that this is an operative concept can be seen in the activities of the Political Work department inside the PLA and the promulgation of its â??Three Warfaresâ?• concept.[24] These include 1) public opinion warfare to influence domestic and international public opinion, 2) psychological warfare to demoralize enemy soldiers and civilians, and 3) legal warfare to gain international support through both international and domestic law. Only the latter element is outside what most people term influence operations or cognitive warfare.[25]

Chinese literature on cognitive warfare (èª•ç?¥ä½?æ?°) is as diffuse as Western research is about influence operations. The volume of Chinese writings on the topic is significant, indicating the emphasis and interest within Chinaâ??s leadership.[26] Recent articles address the value of confrontation via the social media battlefield.[27] Researchers from Chinaâ??s psychological warfare unit call for the PLA to â??speed up the research for online propaganda technology targeted toward the real-time release on social platforms, voice information synthesis technology using deep learning and other technology, as well as online netizen sentiment trend analysis using big data analytics.â?• [28]

One pair of Chinese researchers identified another aspect of intelligent operations in the form of â??cognitive confrontationâ?• (è®¤ç?¥å¯¹æ??), in which the key objective is to achieve decisive supremacy over enemies in terms of information and awareness. They forecast that future operations should attack enemy perceptions and understanding of the battlespace by â??taking the cognitive initiative and damaging or interfering with the cognition of the enemy based on the speed and quality of the cognitive confrontation.â?•[29] Such a struggle will replace traditional warfare concepts that have emphasized control over physical domains such as land, air, and sea. This extends the concept from purely social media manipulation towards an operational application that US military planners may need to worry about.

China has read Clausewitz, and PLA analysts recognize that war â??is ultimately a contest of human will. The key to victory is the ability to impose oneâ??s will on the audience. Cognitive domain warfare takes peopleâ??s will, spirit, and psychology as the goal of confrontation, strengthens oneâ??s own will and weakens the enemyâ??s will.â?•[30] They recognize that modern technology, including generative AI, has increased the ability to target the cognitive domain with â??cognitive ammunition.â?• Yang Cunshe talks of increasing the fog of war for the opponent through cognitive interference, confusion, and blocking in order to increase the likelihood of the opponent making wrong decisions and actions.

The PLA has long extolled â??disintegrating the enemyâ?• via politico-psychological attacks and subversion as a means of undermining an opponentâ??s will to fight.[31] Chinese researchers appear

to be interested in exploring methods of impacting key decision-makers, rather than just the general public. They are also interested in various physical means of targeting and affecting human targets beyond social media and other information systems.

Evidence of this is seen in Chinese military analysts writing about Cognitive Domain Operations, which is defined narrowly and focused on degrading both the military will to fight and generating friction and uncertainty. As one trio wrote:

Cognitive domain operations take the human brain as the main combat space and focus on striking, weakening, and dismantling the enemyâ??s will to fight, using human psychological weaknesses such as fear, anxiety and suspicion as a breakthrough point, focusing on soft-kill methods to create an atmosphere of insecurity, uncertainty and mistrust within the enemy, and increasing their internal friction and decision-making doubts.[32]

Some Chinese writers think in terms of multi-domain operations and creating dilemmas just as US joint doctrine authors do. In this regard, one author admits that physically destroying enemy decision-making centers, command hubs, and early warning systems is necessary. But he goes on to stress the greater need to work at â??soft killingâ?• through cognitive shaping, induction, intervention, and control, by embedding cognitive domain operations into â??hard destructionâ?• efforts to generate an asymmetric advantage.[33]

Some PRC researchers feel that the emerging metaverse will vastly expand the target set and success rate for CDO.[34] Some others write in terms of hearts and minds and impacting the emotions of target audiences.[35] Other scholars are more technologically oriented and see the potential for cognitive enhancement through Brain-Computer Interfaces.[36] As reported by Elsa Kania, the Chinese are interested in more than the employment of modern information technologies. Their research programs include work in brain sciences, human enhancement, biotech, as well as military applications of neuroscience.[37]

Chinese officials do not anticipate that the application of cognitive sciences and technologies will be used only against adversaries. They envision employing these technologies to enhance their own human performance as well. As noted in the CCPâ??s leading theoretical journal:

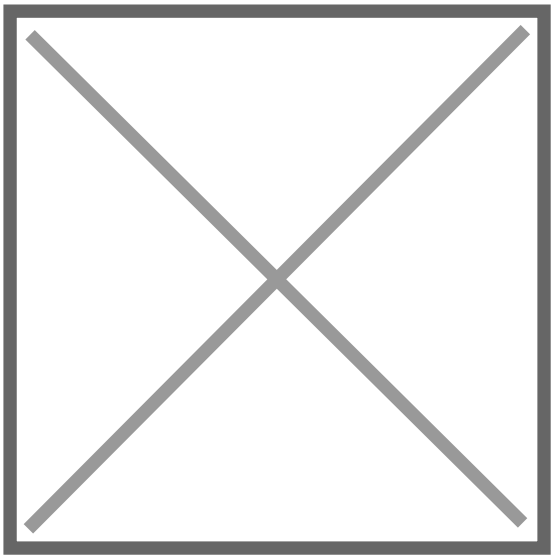
Brain Strengthening is to enhance human cognitive functions by means of neurofeedback technology, electromagnetic stimulation technology, etc., to improve the effectiveness of military training of personnel and enhance their combat capability. Real-time neurofeedback techniques can train and reshape the brain to improve its cognitive functions, thereby enhancing cognitive combat capabilities**.** [38]

Russiaâ??s Version

There is little in the Russian literature that discusses Cognitive Warfare in those terms. However, indirect modes of warfare are a familiar strain in Russian scholarship and practice, including notable writings about â??Subversion Warsâ?? (*Myatezhevoyna)* during the Cold War.[39] Moscow has employed so-called â??active measures,â?• including cyberattacks and disinformation campaigns, as well as limited coercive measures, to advance its interests for generations.[40] The Russian intelligence services are well-practiced in designing and conducting campaigns to utilize coercive actions and information tools.[41] Western analysts tend to divide Russian practice through various lenses, including propaganda, information operations, or disinformation.[42]

The latest wrinkle in Moscowâ??s longstanding practice is the exploitation of social media, which is seen as an extension of the battlespace.[43] Election interference in Europe and the United States is another aspect of this playbook, but a critically important one to deflect if we expect to preserve democratic freedom.[44]

While the term may not be common, the pursuit of cognitive effects is clear. President Putinâ??s advisors brag openly about the Kremlinâ??s influence campaigns. â??Foreign politicians talk about Russiaâ??s interference in elections and referendums around the world,â?• one such advisor stated, but â??In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it.â?•[45] Experts warn that a general understanding of Russiaâ??s malign influence playbook is lacking.[46]



The closest concept to Cognitive Warfare is the Russian concept of Reflexive Control. This has been defined as consisting of â??transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. The goal of reflexive control is to prompt the enemy to make a decision unfavorable to him.â?•[47] This definition notes a key requirement: the need to tailor false information to the specific target, to impact the targetâ??s responses and reactions. Reflexive control involves targeting decision-making through multiple vectors â?? adversary information processing, as well as emotional, psychological, and cultural frames within which decisions are made. Reflexive control appears to have evolved in Russian discussions and is now displaced by perception management.[48]

As early as 2010, influential Russian military authors noted the superiority of Western military power and began to stress the need for more asymmetric approaches.[49] This idea was expanded upon in subsequent articles, which saw a role for information confrontation to disorganize military command and control and state administration.[50] They further extended their thinking to stress the role of non-military attacks in what they labeled the Initial Period of War (IPW). They argued that this period can be decisive in future wars, and that it would include subversive acts, provocations, information operations, and psychological attacks in conjunction with military operations.[51] Their assessments also found that success could be accomplished by the employment of â??military, economic, and IT measures in combination with efficient psychological information campaigns.â?•[52] These authors later argued for a concept called New Generation Warfare (NGW), a â??newâ?• form dominated by â??information and psychological warfare seeking to achieve superiority.â?•[53] The Russian Chief of Staff, General

Valery Gerasimov, expanded on this aspect in his noted talk on future warfare, going so far as stating that â??The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.â?•[54]

There has been a recent link between Russiaâ??s indirect methods and cognitive warfare produced by the Institute for the Study of War (ISW). According to this research, â??The primary objective of Russian cognitive warfare is to shape its adversariesâ?? decision-making and erode our will to act.â?• [55] Their study identifies the multi-modal character of Russiaâ??s disinformation efforts. The Kremlin uses all platforms that transmit information, not just social media, but conferences, international frameworks, diplomatic channels, and influential individuals as means of employing Cognitive Warfare. According to the analysts at ISW, Russiaâ??s version goes well beyond the dissemination of information and includes physical activities in peace, crisis, and war. These physical means include military exercises, sabotage, cyber-attacks, combat operations, and exaggerations of Russiaâ??s military capabilities and battlefield progress.

This was not news to dedicated scholars of the Russian way of war.[56] In both theory and practice, the Russians employ a broader conception of war than most Western states.[57] This includes forms of subversion against political leaders and the general population, as well as other hostile measures that combine physical and cognitive means and effects.[58] Like the Chinese, Russian writers are becoming less concerned with attrition of the opponentâ??s order of battle and increasingly interested in targeting the adversaryâ??s perception and will. To be sure, traditional military means are not overlooked either, as they too can impact perception and will. More recent scholarship highlights the potential impact of Artificial Intelligence on Russian disinformation efforts.[59]

United States

The earliest US author on this topic is James Lewis from CSIS. His in-depth 2018 study of cyber conflict highlighted the generation of what he termed â??cognitive effects.â?• The goal in future conflict, Lewis concluded, â??is not a kinetic effect (achieved with shells and bombs), but a cognitive effect, in other words, manipulating information to change thoughts and behavior. The strategic goal is to influence morale, cohesion, political stability, and, ultimately, to reduce the opponentâ??s will to counteract.â?• [60] His view aligns well with Russian thinking and the PLA.

The US intelligence community has monitored this development as well. In its annual threat assessments, both in 2022 and 2024, the Director of National Intelligence devoted coverage to the evolution of Chinese writings from psychological warfare to CDO, which they describe as combining psychological warfare with cyber operations to shape adversary behavior and decision-making. The

assessment also noted that the PLA is looking at generative AI to generate synthetic media, including deepfakes.[61]

Analysts at RAND have identified Chinaâ??s growing interest in systems and information confrontation.[62] One RAND researcher, Nathan Beauchamp-Mustafaga, has extensively studied the PLAâ??s development of Cognitive Domain Operations.[63]

While the Chinese military seems intensely interested in cognitive warfare, the American professional military journals are fairly quiet. Yet, there have been few articles in the professional journals. One pair of Marine officers wrote about how CDO is tied to Maneuver Warfare because of its emphasis on human will (and presumably psychological dislocation) and argued that â??the United States must develop its approach to CWâ??defensively as well as offensively.â?•[64]

One relatively recent article tied Cognitive Warfare to actions below the threshold of warfare, the so-called â??gray zone.â??[65] This seems to be tied to a very limited reading of both Chinese and Russian publications. The articleâ??s criticism of Joint doctrine was noteworthy, as were its series of recommendations to enhance the readiness of the Joint warfighting community. The subject is not entirely unknown to readers of this journal.[66]

Assessment

There are many and varied definitions of this topic, and its complexity is exacerbated by the nature of the technologies involved, including those in the cognitive and neurosciences. It is further complicated by vague connections to larger conceptions like gray zone tactics and influence operations. The literature is scattered and contains limited evidence on tactics and technologies being considered.

Cognitive warfare could be viewed as a concept that may help promote the cognitive domain and squeeze out â??the ounces of cognitive effectâ?• the JCS Chairman has called for.[67] While I have some reservations about introducing a new term into a crowded field, the term â??cognitiveâ?• is superior to broad terms like information or influence. Psychology is a broad field, and cognition narrows the subject to key features. It directs attention to the target and desired effect. I am less enthralled with the â??warfareâ?• label and think the Chinese terminology is better.

Arguably, some of the effects expected by the conduct of Cognitive Warfare can be conceived as part of the under-appreciated concept of subversion.[68] Some scholars believe we have entered an age of algorithm-fueled propaganda and superpowered subversion.[69] This is a valid term, but it is not traditionally employed in the US military lexicon. A RAND study almost two decades ago found the term vague at best.[70] It has not become any clearer over the last two decades, given the proliferation

of terms.

The term â??cognitiveâ?• is superior to broad terms like information or influence.

Scholars in this field have addressed cognitive warfare as a form of subversion. This would be fine if we limited the concept to non-military targets by non-military forces. The writings and efforts by the PLA and Russian military would beg to differ here and suggest that more than informational subversion is involved.

Subversion is not traditionally seen as a complement or component directed at conventional forces in warfare as understood in the West. It is clear that China and Russia expect to exploit psychological and cognitive effects in wartime as well, and seek to target military decision-making and combat effectiveness. We should expect military formations and their leaders to be targets as well. In short, the employment of cognitive confrontation against national security leaders or military commanders and their staff in wartime does not square with subversion.

If US adversaries were solely oriented on manipulating domestic audiences, a strong argument could be made that labeling this as a form of â??warfareâ?• over-militarizes the problem and distorts the search for solutions that would best address the issue. But as China and Russia use both intelligence and military assets, and seek to target political and military command systems, Cognitive Warfare seems to warrant greater consideration over subversion.

Analytical Framework

To help promote the potential development of this concept, we will need an analytical framework that explains the scope of the cognitive domain and the potential for applications of maneuver/confrontation in that domain. To grasp the potential of cognitive warfare, including its offensive use and appropriate defensive countermeasures, a broader analytical framework was conceived that captures a range of perspectives and authors. This framework helps define the potential scale and scope of the concept and its applications. Figure 2 offers an initial depiction to stimulate discussion and debate.

This framework depicts a larger or more comprehensive conception of cognitive warfare that captures both offensive and defensive contributions. The matrix reflects a continuum of targetsâ??from individuals to collective populationsâ??along the horizontal axis. The vertical axis separates actions and technologies that degrade human cognition (entire lower half of the matrix) from those that enhance individual decision-making (upper left) and those that counter cognitive warfare by improving social cohesions and resilience (upper right quadrant). Along the vertical continuum, political decision-

making processes and military commands are in the middle of the matrix.

Figure 2. Analytic Framework for Cognitive Warfare/Domain Operations

As seen in the literature review, most of the research focuses on cognitive degradation, especially through the manipulation of social media against target societies (lower right quadrant). The majority of PLA authors fall in the lower half of the matrix, emphasizing the projected need to successfully apply information confrontation against a sophisticated, large-scale competitor. But they also include discourse on enhancing human performance and strengthening civil society. Overall, Chinese military authors touch upon every quadrant as opposed to Western analysts, who look at social media manipulation.

The most interesting quadrant is the individual block, which would address how we prepare future leaders to be able to design and conduct campaigns, as well as detect and deflect adversary Cognitive Domain campaigns. In this quadrant, we can conceive of applications of neurosciences and AI-enabled agents to enhance the cognitive function of military commanders and staffs through machine learning and brain-computer interfaces (BCI) of various types.[71] There are advances in BCI technologies that may extend the ability of decision-makers and warfighting operators to make sense of their situational context and make timely decisions.[72] DARPA is funding projects that examine how to augment human cognition via its SCEPTER study.[73] Investments targeting enhanced decision augmentation are represented in this portion of the matrix, as well as defensive measures to thwart neurological weapons and technologies. The legal, moral, and ethical framework for this work should be established first.

The converging role of AI and the neurosciences is going to impact command and control, and should include an ability to detect and deflect adversary CDO.[74]

Revised Definition

Accepting this framework would require some modifications to how we define Cognitive Warfare. Rather than just manipulating or degrading target audiences, the scope of Cognitive Warfare would have to incorporate efforts to develop and attain cognitive advantage at both the individual and collective level, as well as detecting and defending against cognitive domain operations.

This leads to a revision of my original definition: *â??The application of information and cognitive sciences to enhance or degrade the decision-making process and resulting behavior of political and military leaders, and civilian society, in order to obtain a positional advantage in the information environment and designated political objectives*.â?• This is a concise initial stab that can be refined. It is not the final answer, but it does capture the offense/defense or enhancement/ degradation continuum to a greater degree than others.

Revision of Information Operation

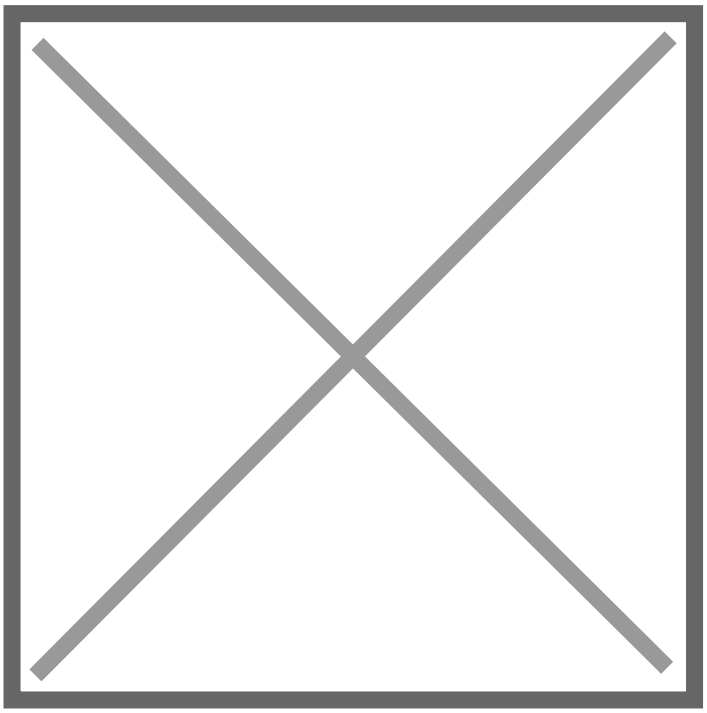
Advancing the concept will face an uphill battle with the existing crowded terminological minefield in information warfare. A conceptual schema for placing Cognitive Domain Operations (CDO) that builds upon the existing joint information operations taxonomy is presented in Figure 3. A few adaptations are embedded in this proposed schema. This deliberately excludes operational security and deception as inherent to sound operational planning. Consideration could be given to including public media engagement for both domestic and foreign audiences. The interface between CDO and MISO needs further study regarding a division of labor. The inclusion of CDO within the joint doctrine pertains solely to the militaryâ??s use of or defense against CDO, and is not intended to suggest applications to domestic contexts.

Figure 3. Relationship of Information Operations and Cognitive Domain Operations

Tomorrowâ??s Cognitive Confrontation

The convergence of physical and moral forces during conflict will continue in this century. The advances in neuroscience, brain sciences, computational technologies, and AI-enabled models have altered the strategic environment and should change how we conceive of and prepare for conflict. These advances have enhanced the ability of competitors to â??expanding the attack surface that foreign adversaries can exploit using cognitive manipulation.â?•[75] As the technological advances in artificial general intelligence (AGI) and machine learning become more operational, they can create mass disruption using low-cost but possibly impactful forms of influence. In the near term, distinguishing between real and manufactured products will become more difficult, if not impossible. The orchestration of physical and cognitive means to generate changes in human behavior and

decision-making will thus accelerate with the advances in cognitive and neurosciences. The eventual development of AGI offers the potential for the perfect storm in Cognitive Warfare. A pro-Chinese influence operation in 2022 involved video content with AI-generated fictitious â??peopleâ?? acting as newscasters, created using artificial intelligence techniques. In the future, competitors will continue to experiment with AI technologies, producing increasingly convincing media that are harder to detect and verify.[76]



Some states will find these technologies uniquely suited to sow divisions and undermine public support in free and open Western societies. Ongoing advances in generative AI will undoubtedly promote the proliferation of deepfakes.[77]

As authoritarian states such as Russia and China exploit these technologies, the global competition in influence or cognitive operations is going to intensify. Studies have identified variation in methods but convergence in narratives between Russian and Chinese foreign information manipulation and interference operations.[78] Veteran intelligence experts believe the United States is losing the battle for cognitive superiority.[79] However, the US government has shuttered intelligence and law enforcement cells and agencies designed to thwart foreign malign information efforts.[80] An objective

assessment of this challenge suggests it is misguided and should be reconsidered. Strategies to address authoritarian influence campaigns, including Cognitive Warfare, need to be developed.[81] Our special operations personnel bring a lot to this arena, coupled with the cyber and information professionals.[82] Embracing the conceptual challenge and addressing capabilities is the first step toward reversing this widening gap.

Conclusion

Information warfare has a long historical foundation in conflict. The concept is linked to our understanding of warâ??s fundamental nature and its essential element of human will. New technologies and methods have altered how information and beliefs can be manipulated to generate effects that impact will and its underlying beliefs, which are producing changes in warâ??s evolving character today. These technologies can also enhance or degrade critical decision-making processes and influence the key contributions that human expertise brings to bear.

Whatever we choose to call it, ignoring our adversaries in this field places the Nation in peril. The United States is presently underprepared to contest intrusions in its information space and will remain so until we recognize the problem and conceive of a more holistic counter approach. Mastering the opportunities and vulnerabilities within the cognitive domain will be increasingly relevant to strategic success in the 21st Century.

Dr. Frank Hoffman retired from the National Defense University in 2024 after 46 years of service in the Department of Defense. He has served in senior executive positions at OSD and the Department of the Navy. He received his Ph.D. from Kingâ??s College, London.

Date Created
2025/12/31