Weaponizing Words: Using Technology to Proliferate Information Warfare

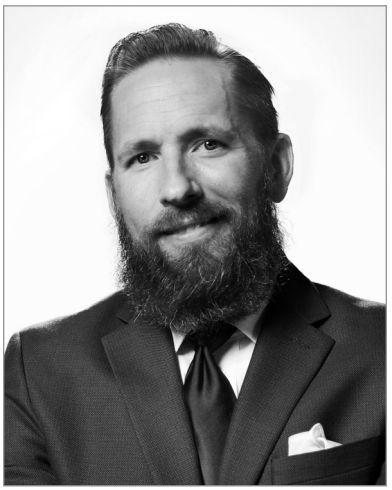
Craig Douglas Albert, Ph.D.
Samantha Mullaney
Lieutenant Colonel Joseph Huitt
Lance Y. Hunter, Ph.D.
Lydia Snider

ABSTRACT

The United States risks losing its information advantage over its near-peer competitors, specifically China. One reason behind this possibility is that the U.S. lacks a coherent doctrine of information warfare, which has put the U.S. at a disadvantage. Considering the Russian interference in elections of several North Atlantic Treaty Organization (NATO) states and allies, including Ukraine, Germany, and, the United States, most stunningly in the 2016 presidential election, this article addresses the question: What is to be done? Before delving into possible solutions, the exact nature of the complex problem must be explored. The purpose of this article is to investigate the ways the U.S. could improve in information warfare, specifically against one of its top near-peer competitors, China. First, this article summarizes how China compares with the United States concerning information warfare and influence operations. Second, it delves into some of the definitional chaos in which the U.S. is mired. Thirdly, the article illustrates the doctrinal and data policies of the U.S. Department of Defense. Finally, it concludes with policy recommendations.

INTRODUCTION

This article asserts that the United States (U.S.) could perform better in the realm of information advantage against its near-peer competitors. Specifically, we examine China's IW (Information Warfare) as it is an increasingly DoD-recognized threat and its growing technological development in the realm of artificial intelligence poses unique threats to the U.S.[1] We demonstrate that the key reason for the current



Craig Douglas Albert, Ph.D., is Professor of Political Science and the Graduate Director of the Master of Arts in Intelligence and Security Studies at Augusta University. His areas of concentration include international relations and security studies, ethnic conflict, cyberterrorism, cyberwar, information operations, and epidemic intelligence. He is widely published, including articles in the *Defense and Security Analysis*; *Iran and the Caucasus*; *Politics*; *East European Politics*; *Chicago-Kent Law Review*; *Politics and Religion Journal*; *Politics & the Life Sciences*; *Cyber Defense Review; Journal of Cyber Policy; Global Society*; and *Intelligence and National Security*. Dr. Albert has testified before a U.S. Congress' joint sub-committee of the House Foreign Affairs Committee. You can follow him on Facebook/Instagram/Twitter @DrCraigDAlbert.

predicament is that the U.S. lacks a coherent doctrine of IW, which puts the U.S. at a disadvantage. China's current advantage is due not to its superior capability, but to the U.S.' lack of clear definition of terms, lack of unified approach, and lack of effective use of data. Thus, the U.S. has the capacity and capability to improve and to regain strategic superiority in this realm. We acknowledge that "information warfare" is not a term currently endorsed and widely used by the U.S. government. In fact, As Ross denotes, the U.S. Army is moving toward a new terminology, contained within the Information Advantage (IA) and Decision Dominance (DD) doctrinal framework.[2] Information Warfare is one of the tasks associated with the IA & DD framework, but we chose to focus on IW to examine an adversary's point of view, and the Chinese Communist party (CCP) is waging information warfare against the U.S.. Also, it is a term commonly used outside the U.S. government and within academia, but we also seek to acknowledge the future of IA & DD in DoD.

As recently as 2018, Seth Jones noted that the U.S. abandoned most of its information capabilities, choosing to focus on lethal rather than political or information operations.[3] Historically, the U.S. has been surprised by its strategic adversaries' sophistication and offensive capability, including non-state actors such as the Islamic State of Iraq and the Levant (ISIS). The Institute for the Study of War acknowledged this in 2016, stating that tactics such as ISIS's virtual caliphate, posed a distinct threat to the U.S. as long as they did not have a clear, government-wide IW strategy.[4] Today, the CCP wields specific information warfare tactics and poses a similar threat.

The U.S.'s IW deficit stems from a lack of a common definition. At times, different units within the U.S. military work against each other, rather than with each other, producing a "silo effect" of data, information, and ultimately intelligence collection and analysis. There is considerable movement within the service branches

Samantha Mullaney is a graduate of Augusta University's Master in Intelligence and Security Studies Program in Augusta, Georgia. The focus of her research is on information warfare forms, tactics, and implications. Her capstone included completing an information warfare internship at the Georgia Cyber Center, where she researched Russian information warfare forms and tactics in Ukraine and the US between 2014 and 2020. Samantha has a BA in History from Fairfield University, an MA in Elementary Education from Boston University, and spent nearly a decade teaching children in Djibouti, Yemen, Jordan, and the UAE. She also speaks intermediate Arabic and basic German. She has been published in *The Cyber Defense Review*.

to adopt and update the language from information warfare and information operations in favor of the term "information advantage." However, many branches are still suffering from a historical lack of common parlance. For instance, when President Clinton established the Broadcasting Board of Governors (BBG), it did not synchronize other elements of public diplomacy or strategic communications, and thus the Departments of State and Defense disseminated different public messaging.[5] Some of this may stem from the fact the Department of State-led Global Engagement Center (which has a vital role supporting information operations) seems to be understaffed, undersourced, and plagued by internal problems that have affected proper messaging in this realm.[6] In fact, Kiesler notes, "There is no recognized leadership to task, direct, resource, or guide policy in the highly complex, disparate field of information operations."[7] LTG Stephen Fogarty and COL (Ret.) Bryan Sparling recently wrote, "The stunning social media-powered rise of ISIS in 2015, Iran's increasing digital belligerence, and China's disinformation surrounding the COVID-19 pandemic" are all examples of information warfare challenges that have begun "a conversation across the defense establishment regarding appropriate roles for the uniformed armed services in this environment of unprecedented information warfare."[8] The above instances of information warfare and information operations (IWIO), as well as Russian interference in several NATO states and allies since at least 2018, begs the question: What is to be done?[9]

Of course, before delving into possible solutions, the exact nature of the complex problem must be explored. The purpose of this article is to investigate how the U.S. is fairing in information warfare, specifically against one of its top near-peer competitors, China. It also seeks to deliver recommendations on how it could do better concluding with specific policies meant to create discussion within the community and mitigate the problems. Before proceeding, however, it is important

LTC Joseph Huitt is a Cyber Warfare Operations Officer, currently serving as Cyber Warfare Deputy Director, Talent Management U.S. Army Cyber Command and also as a senior fellow at West Point's Center for Junior Officers. He is a graduate of the College of Naval Command and Staff, U.S. Naval War College, and a Distinguished Military Graduate of Augusta University. LTC Huitt holds master's degrees in Defense and Strategic Studies, and Intelligence Studies. LTC Huitt has served in leadership positions from the tactical to strategic levels, over his 23-plus years of service. He has gained invaluable experience serving with Special Operations Command in West Africa, USAFRICOM in England, NATO-ISAF in Afghanistan, 66th Military Intelligence Brigade in Germany, USARCENT in Saudi Arabia, 2nd Infantry Division in South Korea, and various stateside units.

to provide some conceptualization of terms that are used throughout this article.

Information warfare (IW) refers to the deliberate use of any element of information to influence the decision making of the adversary and achieve a strategic goal.[10] IW takes place within the information environment, which refers to the physical, informational, and cognitive dimensions that interact with information.[11] Information operations (IO) refer to the specific tactical undertakings in the pursuit of information warfare. The goal of IW is to act in a manner that aids in manipulating the adversary "to win strategic victories and bend the wills of their adversaries without ever engaging in physical combat."[12] It is important to note that IW is used at all stages of warfare, including in kinetic operations. We now turn to a brief illustration of how China dominates the narrative and achieves an advantage across the information environment.

LEFT BEHIND AND OUTMANEUVERED

Malicious actors have benefited from access to modern technology, such as social media platforms, AdTech, and vast troves of stolen data, enabling IW to become one of the cheapest, easiest, and least restrictive types of warfare.[13] The quest to disrupt the decision-making process by using and misusing information is incredibly destabilizing to open societies since IOs target the cognitive domain of individuals and the citizenry as a whole.[14] IW seeks to sow confusion and polarization, thereby destroying the bonds that provide for stability within a society.[15] The U.S.'s historical emphasis on tactical and kinetic activities has placed it at a distinct disadvantage during the current period of conflict between major competing powers, specifically with China.[16] Competing nation-states seek to undermine the U.S.'s democratic norms and stability by utilizing information operations.[17]

Lance Y. Hunter, Ph.D., is Professor of International Relations in the Department of Social Sciences at Augusta University. Dr. Hunter's expertise is in security studies and democratization. Hisresearch focuses on the causes and effects of terrorism and the relationship between evolving technology and conflict. His work has appeared in *Journal of Peace Research*; *Terrorism and Political Violence*; *Party Politics*; *Studies in Conflict and Terrorism*; *Armed Forces and Society; Conflict, Security and Development*; *European Political Science*; *Global Policy*; *Cyber Defense Review*; and *World Affairs*.

China's Strategic Advantage

China possesses a comprehensive doctrine and advanced physical IW assets.[18] This is possibly due in large part to the nature of the totalitarian state, which has more comprehensive control over the information infrastructure than the U.S. and therefore greater strategic advantage.[19] Limited in scope, but strategically long-term, IW measures are consistently implemented, creating a cumulative effect. Chinese IW emphasizes "limited objectives in a limited theatre of operations, conducted away from its borders, higher in tempo, shorter in duration, but highly decisive in nature."[20] By combining the thinking of Sun Tzu and Mao Zedong, Chinese IW is heavily focused on psychology and is used as a weapon in and of itself rather than as a support tool.[21] Most Western scholars define Chinese IW as encompassing China's "three warfares," which include legal, psychological, and media operations. These "warfares" attempt to demoralize the adversary, influence public opinion, and manipulate international law.[22] Most noticeable is China's willingness to use highly integrated IW preemptively, illustrated by its IO campaign against Taiwan.[23] Wortzel explains that China combines electronic warfare, precision strikes, cyber warfare, and attacks on space systems to paralyze an adversary's information capabilities.[24]

Strategically, China adheres to Mao's concept of the "People's War" when waging cyber-enhanced IW. This means utilizing a high volume of cyberattacks or dissemination of disinformation through cyber means. Watts explains the content across platforms is uniform.[25] Furthermore, as a totalitarian state, the CCP can coerce numerous Chinese citizens to do their part and espouse a narrative on behalf of the state, as illustrated by the "50 Cent Party."[26] One advantage is the sheer number of people the CCP has working in this arena. They have the ability to direct vast numbers of actual users to execute bot-like operations. Unlike actual bots, however, these are immune to platform bot

Lydia Snider works for the U.S. Department of the Army as a specialist in foreign malign influence.

violation rules, because behind the accounts are real people. While thousands may be posting at the behest of the CCP, even copying and pasting the same response, when the platform AI studies the event, it sees numerous real accounts, not a bot network. IW is at the forefront of China's revolution in military affairs and is viewed as the critical weapon rather than a support for other military endeavors.[27] China recognizes that it cannot compete with U.S. defense spending and instead, starting in the 1950s, has institutionalized IW which has developed into a Strategic Support Force (SSF), the current central element of China's IW capabilities.[28]

China has created entire institutions to develop IW capabilities, including the Academy of Military Sciences Military Strategy Research Centre, the PLA Academy of Electronic Technologies, and the Xian Politics Academy that trains psychological warfare officers.[29] Additionally, the PLA has utilized simulation training for IW for more than a decade.[30] Psychological warfare units are dispersed throughout the PLA following initial training, providing a common language and doctrine across departments. Additionally, Elsa Kania and John Costello, as well as Larry Wortzel note that China's view of IW subsumes cyber warfare.[31] Given the totalitarian control the CCP needs over the domestic population, this sort of integration of cyber and information capabilities in the international arena would not be out of character. In fact, the control over information and therefore ideology, whether through cyber-mediated elements or not, "may allow for better planning, acquisition, and operations while enabling the creation of a more flexible cadre of personnel tailored toward new paradigms of information operations."[32] China's global network of influencers illustrates this strategy.[33] In this strategy, videos of mostly young Chinese women speaking in the language of the target audience speak of their respect for the target country and its culture and of China as a good friend. These videos appear in over a hundred different languages with almost the same script.[34] Each

of these academies and centers gives China a probable advanatage over the U.S. in that they are steadily increasing their understanding of TTPs in the realm of information warfare and have wide dispersion capabilities as well. The resulting strategy allows for more flexibility and fluidity in its offensive operations.

The last two decades have seen China attempt to move from confrontational IW to the appearance of cooperation.[35] However, the facade has grown very thin in recent years with the development of the "wolf warrior diplomacy" strategy, which vigorously targets the U.S. and other Western nations and institutions.[36] China builds the facade through a proliferation of Confucius Institutes, hosting new journalists from Africa in training workshops, and promoting tourism and events for foreign elites.[37] The Belt and Road Initiative is presented as economic cooperation for the betterment of developing states, but large-scale Chinese investment in Africa has led to negative consequences. The CCP's infrastructure investment, a core element of the Belt and Road Initiative, is directly linked to undercutting local construction companies, operating on a profit margin of less than 10 percent, and is often tied to selection and use of Chinese contractors.[38] In addition, these single-source projects often are launched without feasibility studies or may include a clause to allow for a loan's cancellation and immediate repayment.[39] Although the Initiative is presented as a cooperative endeavor, one is reminded that it is indeed another form of Chinese propaganda, aimed at promoting the overall aims of the CCP.

The Chinese strategy focuses on weakening the institutions that stabilize American society by co-opting human networks inside these institutions. Other CCP-backed groups include the Chinese Students and Scholars Association and the China Association for International Friendly Contact. The former is a network across universities that receives funding from the CCP and distributes propaganda targeted at universities where there may be negative narratives about China.[40] The latter organization specifically targets business people and veterans and seeks to shape messaging through invitations to tour China.[41] When China faces an inability to create a façade of cooperation, it relies on different elements of the three warfares to coerce or manipulate adversaries. This is most adeptly seen in China's activity in the South China Sea.[42] China's aptitude in IW is clear. Its fleet of spy ships, SIGINT stations located as far afield as Cuba, its own dedicated SIGINT/EW aircraft, and dispersed human asset network allow it to carry out IW simultaneously along multiple fronts.[43] In terms of media warfare, China has adroitly co-opted media outlets around the world through its front organization, Xinhua News. In Africa especially, this co-option of local journalists has weakened any concerted critique of China's Belt and Road Initiative and extractive policies, helping China wage a psychological war and also enabling the manipulation of Africa's legal structures.

There is little distinction between foreign and domestic media control by the Chinese Communist Party. For example, the Central Propaganda Department controls China National Radio, China Radio International, and CCTV. Consolidating media control is a deliberate attempt to unify domestic and international propaganda narratives.[44] The United Front, Confucius Institutes, and wealthy Chinese working on behalf of the CCP have co-opted universities,

professors, think tanks, multinational corporations, and researchers to convey to the public crafted messages on behalf of the CCP, funnel research to China, and censor scientific or academic research that would negatively affect China's reputation.[45] This use of messaging encourages Americans to trust the espoused narrative because it comes from traditionally venerated U.S. institutions, such as universities and think tanks. This creates a unified front within China, where the domestic and international narrative focuses on Chinese supremacy, posing a threat in itself to the effectiveness and longevity of democratic states worldwide. The more people "believe" in China's regime, the more a threat is posed to democratic institutions worldwide, in the long run. This is yet another angle China uses in its information war against the U.S.

Chinese IW is also present on social media platforms. Scott Harold, Nathan Beauchamp-Mustafaga, and Jeffrey Hornung posit that China's use of social media helps it destroy an adversary's command authority through the demonization of a leader and the demoralization of the public.[46] Like Russia's, Chinese IW sees chaos and division as a product of successful psychological warfare, whether waged on social media platforms or through strategically placed individuals parroting a Chinese narrative. Given the totalitarian nature of the CCP, any and every business or actor inside of or connected to China can and may be used for the benefit of the state. One advantage the CCP maintains over the U.S. is its willingness to exert state control over social media platforms, through its censorship of internal conversation and with state control over the now internationally used platform, TikTok. With TikTok, the CCP has a platform that both collects data on users and over which it has complete control of what content is delivered to users.

Currently, China's use of cyber for IW is coupled with a powerful and far-reaching network of human agents cultivated through organizations such as the United Front that help execute highly complex and integrated influence operations.[47] This vast network of human assets in multiple arenas enables China to alter public perception and portray messages favorable to the CCP. Specifically, China targets personnel and institutions with financial incentives to dampen negative publicity.[48] The CCP's response to the COVID pandemic is illustrative of its IW capabilities and its strong coordination between overt and covert IW.[49] Now that a brief case analysis of China's use of IW and IO has been illustrated, it is necessary to understand how and in what ways the U.S. lags behind China in the IW/IO competition. Ultimately, the U.S. cannot replicate the CCP's power over the PLA and utilize its IW forms and tactics without demolishing national and international war standards. That does not mean the U.S. cannot find a way to counter these tactics and maintain democratic norms.

DEFINITIONAL CHAOS

The U.S.'s competitors and near-peer competitors have institutions devoted to the successful utilization of information operations and achievement of strategic advantage in this domain. They also have broad, but useful, definitions of IW. Largely, the U.S.' adversaries define IW as conflict in the information space that forces a specific decision by undermining political, information, social, or economic systems, often using mass psychological tactics to destabilize

society by targeting a population.[50] The goal of modern IW against the U.S. is to erode trust in authority and institutions, thereby undermining shared values.[51]

The U.S. government does not have a consistent definition of what IWIOs are, and lacks a dedicated institution or agency with which to wage IWIOs effectively for strategic advantage.[52] IW is divided across multiple agencies in the U.S., such as the Department of State's Global Engagement Center, the CIA, U.S. Cyber Command (USCYBERCOM), and other elements of the military.[53] Essentially, the U.S. uses the "same terms differently in different contexts," which creates confusion and a lack of strategic capability.[54] Scholars such as Whyte define IW as the use or abuse of information to influence the decision-making options and processes of the adversary to achieve military or strategic gains.[55] This is a broad definition that encompasses many tactics within the military and non-military realms. The Army's definition is somewhat similar, noting that IW is a simultaneous effort directed at creating a specific effect in the information environment and is a battle "*of* information," rather than just a battle *for* information.[56] However, a 2012 joint publication from the Joint Chiefs of Staff confined IOs to military operations.[57] In fact, Alicia Wanless and James Pammet note that the U.S. interprets IW/IO in largely military terms and tries to delineate between acceptable and unacceptable actions within these parameters.[58] There is no such distinction for foreign adversaries given their different governing structures.

It is understandable that the military focuses on command and control and how IW targets critical military elements necessary to gain a military strategic advantage. However, the IW waged against the U.S. is far broader than this focused definition. IOs target the cognitive domain of individuals and the citizenry as a whole.[59] China utilizes persistent narratives that cause members of the target society to question themselves, and China seeks to disrupt the decision-making process of a state by using and misusing information. The U.S. government requires a common definition of IW which can be disseminated to national security agencies, the military, and public relations elements. These terms should be clearly defined and the parameters demarcated. The U.S. cannot wage an effective defensive information war without a consistent definition of IW.[60] This article now proceeds to a discussion regarding how the DoD understands and effectuates IW. After detailing this, this article proceeds to set-forth policy recommendations that seek to bolster the U.S.'s IW/IO.

DATA AND THE DEPARTMENT OF DEFENSE

To better understand the impact of information warfare and the U.S. Government's (USG) approach to counter adversary actions, it is imperative to review the existing doctrine and policy that guide it. This article highlights the current guidance from the DoD and some of the challenges of wading through the vast data, directives, and policies which reference decades-old policy, include conflicting guidance, and lack of a common lexicon. To set some common ground, the authors first discuss what DoD defines as data and how this is used to generate information and intelligence. Armed with the understanding that U.S. adversaries and competitors are waging IW, this section outlines the basics of how DoD processes data.

DoD highlights in its Data Strategy that "data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage."[61] Joint Publication (JP) 2-0 highlights that raw data must be collected and by itself may not be relevant or useful. As JP 2-0 further illustrates that information consumed solely by itself may be utilized by a commander, but is not of much use for decision dominance. When related to the operating environment and considered in the light of past experience, however, it gives rise to a new understanding of the information, which may be termed *intelligence*."[62] The intelligence directorate enriches information by collecting national tactical means to answer a commander's requirements, enabling decision dominance. DoD made information the seventh joint function in 2017 based on 2016 guidance first established in Joint Publication 1, "Operations in the Information Environment (IE)."[63]

Publicly available information (PAI) is information available on the open Internet and it plays an important role in IW/IO. DOD Directive 3115.18, "DoD Access to and Use of PAI," issued in 2019, outlines the lawful and appropriate access to "obtain, and use PAI to plan, inform, enable, execute, and support the full spectrum of DoD missions."[64] While new directives are important, old directives have not always been updated, causing confusion and gaps in strategy implementation. The U.S. Intelligence Community (IC) is flush with data; however, it is generally just white noise. Because of the definitional chaos of IO,[65] and the silo effect of data, different U.S. agencies approach IWIO differently and are often at odds with one another. Different units across all branches of the military often look at the same data for different issues and do not share the information across the DoD. In many instances, different military organizations are buying the same data from companies under different contracts for each organization. In other words, there is such a disunity of approach in data collection because DoD has not created a data governance entity to manage data acquisition from private industry and make it available across the force. DoD has put the onus on components to develop and implement their own data acquisition plans.[66] Furthermore, if DoD had a data lake that housed curated, publicly and commercially available information, which was available to its components, it would drastically reduce redundant data as a service contracts. This situation is one of the reasons the U.S. is behind the curve relative to China concerning the information domain and battlespace. This strategic adversary has clear conceptual approaches to influence operations, and has a more centralized or unified approach to information warfare and intelligence collection than does the U.S..[67] Thus, a more unified approach will help connect the dots with the U.S.' collected data. It should be noted that the IC has the data at hand but does not always efficiently utilize the data to achieve its ends. As the U.S. plans for future data acquisition it needs to follow its adversaries' lead in tracking narratives in the languages in which they are communicating and bringing on language and cultural experts who understand the nuances of those narratives.

LACK OF A UNIFIED APPROACH

DoD understands the challenges of IW and has developed numerous policies to attempt to address them with the end state of achieving information advantage.[68] However, these new

policies failed to provide guidance that would benefit DoD organizations and military branches in the twenty-first century. Despite the existing elements of known national power, diplomacy, information, military, and the economy (DIME), and the aforementioned new policies for DoD, the military branches have developed their own approaches that are not synchronized. The term "IW" is also a point of contention—DoD prefers the term (IO), which encompasses a host of information-related capabilities (IRCs).

DoD has published Joint Publication (JP) 3-13, "Information Operations," in 2012 and updated it again in 2014. The definition of IO outlined in JP 3-13 is "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[69] JP 3-13 further discusses that, after analyzing a target audience, desired effects can be accomplished through various means, including DIME actions. Here, the lack of a unified approach becomes apparent as these IRCs are managed separately at the joint level and across all military branches. For context, IRC capabilities can include but are not limited to personnel from the electronic warfare (EW), cyberspace operations (CO), military information support operations (MISO), civil-military operations (CMO), military deception (MILDEC), intelligence, and public affairs (PA) communities.[70]

All the communities mentioned above have developed their own guidance over time, executed it with various authorities, and achieved varying degrees of success. Some of these capabilities are nascent (i.e., cyber), and others have a long tradition (i.e., MILDEC). Historically, it is challenging for DoD to synchronize all these capabilities beyond incorporating them for a specific operation. However, the U.S. Congress has noticed that the environment has changed and identified gaps in its understanding of combating the *shaping operations* U.S. adversaries are conducting within the information environment.

To summarize, the U.S. is behind its strategic near-peer competitors, specifically China, due to the lack of a clearly implemented and unified approach, definitional chaos within the information environment, and inefficient utilization of evolving data and information into intelligence. With the understanding of Chinese influence operations and an illustration of the precise reasons the U.S. is behind its strategic adversaries based on DoD doctrine and implementation, what is to be done?

POLICY RECOMMENDATIONS AND DISCUSSION

The first and most obvious policy recommendation is that the U.S. needs to form a centralized, unified approach dedicated to data, intelligence, and IW. This has already been achieved by the CCP. Although there are some in the U.S. who may oppose the creation of such a plan, this article demonstrates why it is a strategic necessity. The U.S. is losing because of its inability to turn data into operational intelligence and its lack of human capital allocation regarding IW. This gives its adversaries the strategic advantage. What is not necessarily needed is a

centralized entity to develop a unified approach. Rather, it is a unified approach based on policy across departments and within a unified command structure.

Existing institutions may provide the backbone from which to consolidate and then disseminate a unified approach to IW. Sue Gordon and Eric Rosenbach argue in *Foreign Affairs* that the Cybersecurity and Infrastructure Security Agency should become the center of gravity for domestic cybersecurity operations.[71] Additionally, they argue that USCYBERCOM ought to be realigned and re-envisioned into something approaching the U.S. Special Operations Command (USSOCOM). In a similar vein, Lieutenant General Timothy D. Haugh, Lieutenant Colonel Nicholas J. Hall, and Major Eugene H. Fan argue that this new information environment requires "tight partnerships among all elements of the DoD, the interagency, and our coalition partners, driving a shift in the weight of effort from preparing for conflict to competing now." They continue, "We do not need a new approach to command and control, but a new framework that both materially creates the awareness among, and organizes the horizontal coordination of, organizations across the continuum of cooperation, competition, and conflict."[72] Regardless of whether a unified approach creates a new entity or reenergizes current entities with new authorizations to handle all aspects of IWIO, this is the first step to help the U.S. counter IWIO by adversaries. It is currently unclear if the upcoming redefinition of terms by the Army, and its switch to using information advantage rather than information operations, as recently noted by Ross, will help or hinder the operational chaos produced by the terminology.[73]

Secondly, once a unified approach is defined, the U.S. needs to develop clear operationalizations and definitions for its information operations and strategic approaches. These concepts need to be clearly codified and implemented across the board, intra- and interagency. Once this is done, it may be necessary to go on the IW offensive. The U.S. needs to set the narrative in several key areas in an assertive way, using digital and social media in a fashion similar to how Radio Free Europe was used in the Cold War to communicate pro-democratic and anti-communist messages to thousands of individuals living behind the Iron Curtain.[74] The advantages and strengths of democracy, democratic participation, and respect for human rights need to lead the agenda-setting program of the U.S..

Currently, the U.S. is playing defense concerning the democratic narrative and, in fact, is generally reactive in response to disinformation and propaganda. There is almost no chance of winning the influence war within the Chinese space if the U.S. does not utilize successful tactics. Justin Sherman explains in a prior article for CDR that the Chinese have built out "variously undemocratic practices, such as online censorship, using digital technologies."[75] However, he also notes that digital authoritarianism affects the international arena, and U.S. national security directly, by allowing authoritarian regimes to consolidate power, encouraging the global diffusion of digital surveillance and propagating the idea of Internet sovereignty, thereby potentially avoiding U.S. deterrence strategies.[76] Thus, authoritarian spaces control the information environment and, conversely, the information environment helps proffer authoritarianism.[77] Playing constant defense is a poor strategy and has been largely unsuccessful for

the U.S. Our near-peer competitors' sophistication demands the return to strategic offense in the information environment.

Furthermore, the U.S. must strengthen its defenses. For instance, U.S. policy typically does not allow for individuals within the IC or IWIO domains to engage with fake accounts, bots, or organized campaigns aimed at the U.S. citizenry. In fact, according to Major Jessica Dawson, "The result of this is that there is no agency within the Army charged with understanding the ways in which U.S. adversaries can manipulate the domestic information warfare space... [T]he U.S. Army is unable to assess or respond to threats in the social media space."[78] Although it may draw more attention to these accounts and issues, which the U.S. typically discourages, counter-attacking or taking the offensive may surprise Chinese information operatives. If done in a sophisticated manner, U.S. intervention into these spaces may quickly throw its adversaries into an emotive state, which could derail their policy. The action would also signal a policy and strategic culture shift in the U.S., which could help reassert U.S. dominance in this information space, forcing adversaries to play its game, rather than vice versa.

Additionally, U.S. near-peer competitors use popular influencers to their strategic and cultural advantage.[79] China pushes out influencers targeting its own population, and it hires Western influencers to target the West. In fact, China targets its own population through data-driven analytics to exert domestic control.[80] The U.S. could use a similar methodology against China and foreign adversaries as well, without violating U.S. law, military norms, or democratic codes of conduct. Instead of shutting down DoD military influencers, the U.S. could help them expand to combat Chinese IW/IO. Military members not on TikTok could be used to counter CCP efforts stateside by explaining why they are not on the platform. Active social media influence by exceptionally talented individuals could act as an IWIO deterrence. As Morin states, domestic IIOs would be targeted toward adversarial IIOs and seek to reduce "the viewing of an adversary's IIO content."[81]

As the digital age progresses and the information environment becomes a clearinghouse for great power conflict, the U.S. needs to engage this domain strategically and tactically. It can do so by setting its own agenda in this space, while also remaining dedicated to liberal democracy.[82] As noted earlier, Chinese IWIO strategies focus on active offense at all times; there is no difference in their peacetime versus conflict strategies. To compete within this space, the U.S. needs to choose wisely which elements of IW should be used offensively. David Morin explains that incorporating Information Influence Operations (IIOs) into USCYBERCOM tactics "would allow [the U.S.] to effectively guide perception and even shape the targeted population's perception of reality, if effectively conducted."[83]

The U.S. should also consider its strategic use of the Internet in multiple areas. In terms of web presence on the domestic front, all government sites should be technologically savvy and well-integrated with social media platforms to help bolster government legitimacy among generations that are increasingly technologically-oriented. Additionally, the government should

consider policies and procedures that would enable the exclusion of bad foreign actors, companies, and advertisement funding.[84] If the U.S. were to disrupt and deny foreign actors' abilities to disseminate influence operations actively through U.S. companies and Internet platforms, it would begin the process of active defense.

Due to China's regime structure, the U.S. and China are playing two separate games with separate rule books. China is directly targeting U.S. civilian interests, has deep pockets to spread its message, and has control of its own media. It can even pay U.S. companies for advertising space, whereas the U.S. denotes limited funds to IW/IO and does not focus on the same targets. The U.S. should utilize the Internet in a manner that aggressively goes on the offensive on behalf of American citizens. This will likely encourage China to complain that the U.S. has caused offense on the international stage. However, it is long past time for the U.S. to demonstrate clearly its IWIO capabilities and impose costs on its adversaries in their attempts to disrupt American society.

For this to be effective, the U.S. must engage in IWIO through a whole-of-society approach, but one that plays out much differently than the centrally directed, coercive manner of authoritarian regimes. Although this article argues that DoD needs a centralized division and strategy for IW/IO to compete with China, it also needs a decentralized environment which allows for all sectors of U.S. society to engage in the game by their own initiative. This would include defense, entertainment, schools, and the citizenry, as imagined by researchers Cristina-Elena Ivan, Irena Chiru, and Rubén Arcos.[85] The U.S. needs an overarching message to disseminate and, to be effective, it has to come from multiple segments of society. As a part of this whole-of-society approach, U.S. companies will need to play an active role. As Dawson notes, technology companies such as Facebook and Google are ungoverned, unrestricted spaces; as such, they pose a significant security risk for the United States, especially concerning data and intelligence for IOs.[86]

The focus of technology platforms should be to prevent U.S. adversaries from co-opting the platform to wage a disinformation campaign against the U.S. citizenry. Most especially, as Major Dawson insists, "The U.S. must recognize the current advertising economy as enabling and profiting from information warfare being waged on its citizens and address the threat."[87] While we must address the fight the adversaries put in front of us, we win, not by trying to play their game, but by playing ours effectively.

DISCLAIMER

The views presented are those of the author(s) and do not necessarily represent the views of DoD or its components.

NOTES

1. Lily Hay Newman, "It's Time to Get Real About TikTok's Risks," *Wired Magazine* (September 6, 2022), https://www.wired.com/story/tiktok-nationa-security-threat-why/.
2. Lieutenant Colonel Robert J. Ross, PhD, "Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations," *The Cyber Defense Review* (Fall 2021): 63.
3. Seth G. Jones, "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare," CSIS (October 1, 2018) https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.
4. Harleen Gambhir, "The Virtual Caliphate: ISIS's Information Warfare," *Institute for the Study of War* (December 2016), https://understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf
5. Lieutenant Colonel Gregory M. Tomlin, PhD, "The Case for an Information Warfighting Function," *Military Review* (September-October 2021): 91, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-21/tomlin-info/tomlin.pdf.
6. P Jack Kiesler, "A Next Generation National Information Operations Strategy and Architecture," Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (September 13, 2021), https://www.belfercenter.org/publication/next-generation-national-information-operations-strategy-and-architecture.
7. Kiesler, A Next Generation, 8/36.
8. Lieutenant General Stephen G. Fogarty and Colonel (Ret.) Bryan N. Sparling, "Enabling the Army in an Era of Information Warfare," *The Cyber Defense Review* (Summer 2020): 18.
9. Connor Cunningham, "A Russian Federation Information Warfare Primer," The Henry M. Jackson School of International Studies, University of Washington (November 12, 2020), https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.
10. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, "Introduction" in *Information Warfare in the Age of Cyber Conflict*, edited by Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, 1-11.
11. See *DOD Dictionary of Military and Associated Terms,* (as of January 2021), and DOD Directive 3600.01, *Information Operations (IO)*, (May 2, 2013, incorporating Change 1, May 4, 2017), and GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C., October 18, 2019), and Congressional Research Service, *Information Warfare: Issues for Congress,* R45142 (updated March 5, 2018).
12. Scott D. McDonald, Brock Jones, and Jason M. Frazee, "PHASE ZERO: How China Exploits It, Why the United States Does Not," *U.S. Naval War College Review* 65, 3 (Summer 2012) https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1471&context=nwc-review.
13. Justin Sherman, "Digital Authoritarianism and Implications for US National Security," *The Cyber Defense Review* (Winter 2021): 108-109.
14. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, eds., *Information Warfare in the Age of Cyber Conflict* (New York: Routledge, 2021), 237.
15. Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service Report* (2018): 1.
16. Mark Pomerleau,"Why is the United States losing the information war?" *C4ISRNet* (October 2020): 5, https://www.c4isrnet.com/information-warfare/2020/10/05/why-is-the-united-states-losing-the-information-war/.
17. Pomerleau, "Why is the United States?"
18. Manuel Cereigo, "China and Cuba and Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyberwarfare," www.lanuevacuba.com/archivo/manuel-cereijo-123.htm.
19. Theohary, *Information Warfare.*
20. J. Yin and P.M. Taylor, "Information Operations from an Asian Perspective: A Comparative Analysis," *Journal of Information Warfare* 7, no. 1 (2008), 3.
21. Yin and Taylor, "Information Operations, 3.
22. Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *US Army War College, Monographs, Books, and Publications* (2014): 30, https://press.armywarcollege.edu/monographs/506.
23. J. You, "China's Emerging National Defence Strategy," *China Brief* 4, no. 23 (2004): 5-7, http://jamestown.org/china_brief/article.php?issue_id=3152.
24. Wortzel, "The Chinese People's," 13-15.
25. Watts, "China's Propaganda."https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/.

NOTES

26. Renee Diresta et al., "Telling China's Story: The Chinese Community Party's Campaign to Shape Global Narratives," Stanford Cyber Policy Center, Stanford Internet Observatory (2020): 14.
27. Yin and Taylor, "Information Operations," 3-4.
28. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (2018): 106; Kania and Costello, "The Strategic Support Force," 116.
29. Yin and Taylor, "Information Operations," 4.
30. Timothy Thomas, "The Chinese Way of War: How Has it Changed?" The MITRE Corporation, sponsored by U.S. Army Futures and Concepts Center (2020): 47.
31. Kania and Costello, "The Strategic Support Force," 111; Wortzel, "The Chinese People's," 16.
32. Kania and Costello, "The Strategic Support Force," 112.
33. Lili Turner and Nirit Hinkis, " Chinese State Media's Global Influencer Operation," Miburo (now part of the Digital Threat Analysis Center), (January 31, 2022) https://miburo.substack.com/p/csm-influencer-ops-1
34. Turner and Hinkis, " Chinese State Media's."
35. Yin and Taylor, "Information Operations," 5.
36. Ben Smith, "Meet Zhao Lijian, The Chinese Diplomat Who Got Promoted for Trolling the US on Twitter," BuzzFeed News (December 2, 2019), https://www.buzzfeednews.com/article/bensmith/zhao-lijian-china-twitter.
37. Maddalena Procopio, "The Effectiveness of Confucius Institutes as a Tool of China's Soft Power in South Africa," *African East-Asian Affair*s (2015): 1-2.
38. Reuben L. Lifuka, "Corruption in the Zambian Construction Sector: The China Factor," The Hoover Institution, *China's Sharp Power in Africa* (2021): 6, https://www.hoover.org/sites/default/files/research/docs/lifuka_webreadypdf.pdf.
39. Lifuka, "Corruption," 8.
40. Watts, "China's Propaganda."
41. Wortzel, "The Chinese People's," 33.
42. Doug Livermore, "China's 'Three Warfares' in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, March 25, 2018, https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.
43. Yin and Taylor, "Information Operations," 7.
44. DiResta et al., "Telling China's Story," 9; Wortzel, "The Chinese People's," 32.
45. Alex Joske, "The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System," Australian Strategic Policy Institute (June 9, 2020), https://www.aspi.org.au/report/party-speaks-you; Wortzel, "The Chinese People's," 32.
46. Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, "Chinese Disinformation Efforts on Social Media," RAND Corporation (2021): 21.
47. DiResta et al., "Telling China's Story," 3, 7.
48. Theohary, *Information Warfare*, 12.
49. DiResta et al., "Telling China's Story," 39.
50. Ivan, Chiru, and Arcos, "A Whole of Society," 498; Lin, "On the Organization," 167.
51. Ivan, Chiru, and Arcos, "A Whole of Society," 495; See also Chris Dougherty, "Confronting Chaos: A New Concept for Information Advantage," *War on the Rocks*, September 9, 2021, https://warontherocks.com/2021/09/confronting-chaos-a-new-concept-for-information-advantage/.
52. Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD," *The Cyber Defense Review* 5, no. 2 (2020), 90.
53. Theohary *Information Warfare*, 7.
54. Lin, "Doctrinal Confusion," 100.
55. Whyte et al., *Information Warfare*, 2.
56. FM 3-13: *Information Operations*, Department of the Army, Headquarters (December 2016), 2-1, http://www.apd.army.mil; Zac Rogers,"The Promise of Strategic Gain in the Digital Information Age: What Happened?" *Cyber Defense Review* 6, no.1, (Winter 2021): 87.

NOTES

57. *Information Operations,* Joint Chiefs of Staff, Joint Publication 3-13 (November 27, 2012): vii.
58. A. Wanless and J. Pamment, "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18, no. 3 (Winter 2019): 7.
59. Whyte et al., *Information Warfare,* 237.
60. Wanless and Pammet, "How Do You Define a Problem Like Influence?" 9.
61. DOD, *Executive Summary.*
62. Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence* (October 22, 2013).
63. Joint Chiefs of Staff, *Joint Publication 1: Doctrine for the Armed Forces of the United States* (March 25,2013), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jpl_ch1.pdf.
64. DOD, *DOD Access to.*
65. Wanless, A. and J. Pammet, "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18, no. 3 (Winter 2019): 2.
66. DOD, *Executive Summary.*
67. See Tashev Blagovest, Lieutenant Colonel Michael Purcell, and Major Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU* Journal 10, no. 2 (2019): 133.
68. See GAO, "Information Operations: DOD Should Improve Leadership and Integration Efforts," GAO-20-51SU (October 2019) for a complete breakdown of terms the DOD uses.
69. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (2014).
70. *Ibid.*
71. Sue Gordon and Eric Rosenback, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs* 101, no.1 (2022): 10-20.
72. Lieutenant General Timothy D. Haugh, Lieutenant Colonel Nicholas J. Hall, and Major Eugene H. Fan, "16th Air Force and Convergence for the Information War," *The Cyber Defense Review* 5, no.1(2020): 41.
73. Robert J. Ross, "Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations," *The Cyber Defense Review,* 6 no. 4 (Fall 2021): 63-73.
74. McCauley, Russian Influence Campaigns, 475; See also, Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Difference,* Institute for National Strategic Studies Strategic Perspectives, no. 11 (Washington, DC: National Defense University Press, 2012): 12-97.
75. Sherman, "Digital Authoritarianism," 107.
76. Ibid.
77. Ibid.
78. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6, no. 1 (2021): 63-79.
79. David Morin, "Information Influence Operations: The Future of Information Dominance," *The Cyber Defense Review* 6, no. 1 (2021): 136.
80. Dawson, "Microtargeting as Information Warfare," 68.
81. Morin, "Information Influence Operations," 137.
82. Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *The Washington Quarterly* 43 no. 2 (2020): 75-96.
83. Morin, "Information Influence Operations," 136.
84. Dawson, "Microtargeting as Information Warfare."
85. Ivan, Chiru, and Arcos, "A Whole of Society."
86. Dawson, "Microtargeting as Information Warfare," 64.
87. Ibid.