Doctrinal Confusion and Cultural Dysfunction in DoD

Regarding Information Operations, Cyber Operations, and Related Concepts

Dr. Herbert Lin

ABSTRACT

The doctrinal history of information operations, cyber operations, and psychological operations within DoD is tangled and confused. Moreover, those military specialties rank lower in the DoD pecking order, and those with such specialties are accorded less respect than those specializing in traditional combat arts. These two realities have led to inconsistent usage of these and related terms within DoD and the larger national security community in government as well as in public discourse and, arguably, a misallocation of resources given the importance of the information environment in military operations.

1. INTRODUCTION

In a Lawfare posting earlier this year,[1] I asked how cyber operations, which are the bread and butter of U.S. Cyber Command's (USCYBERCOM) operational activities, could be regarded as psychological operations. This question was raised by two recent articles on NPR[2] and in *The Washington Post,*[3] the former discussing past activities of USCYBERCOM and the latter discussing possible future activities. Both articles described these activities as "information warfare," "information operations," "psychological operations," and "influence operations." One obvious question raised by these reports is this: In what sense should these activities USCYBERCOM is contemplating or conducting be considered any of these things?

To the extent these operations seek to influence the behavior of senior Russian or ISIL leadership, they are clearly influence operations. Perhaps the fact that they use information to do so makes them information operations. The influence is psychologically mediated; hence they could be psychological operations. They are enabled by cyber operations that use computer hacking techniques to locate, identify, and possibly manipulate the sensitive personal data of the targeted individuals. Maybe they are information warfare activities, since they seek to respond to an information warfare campaign Russia has waged against the United States and its democratic institutions for a very long time (but first burst into public view during the 2016 Presidential election). On the other hand, *The Washington Post* story was careful to note that the options being considered did not "envision any attempt to influence Russian society at large"—thereby excluding one common understanding of what some of these terms often mean.

These terms sometimes are used interchangeably in public discourse and even within the Department of Defense (DoD) community, but they are not synonymous. These terms also have a confused and tangled history even within the DoD. Some have formal definitions, but in practice and reflecting that tangled history, even those working within DoD do not use them consistently in communicating among themselves or with the public. This inconsistent usage creates confusion within the U.S. Government and within public discourse as well.

2. ON DOCTRINE, CONCEPTS, AND TERMINOLOGY

This section reviews in some detail the emergence and evolution of a variety of DoD concepts and terminology relevant to information and information technology systems as reflected in joint doctrine, which is widely regarded as the most authoritative source for the meaning of various terms and how they are used to describe US military thought. "Most authoritative" however, does not always mean entirely coherent or consistent. The complexity of DoD doctrine is such that its various parts evolve at different rates, and hence, over time, doctrine may well suffer from at least a partial lack of synchronization.

Herbert Lin is senior research scholar for cyber policy and security at Stanford University's Center for International Security and Cooperation and the Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in offensive cyber operations and the security dimensions of information warfare and influence operations. Dr. Lin is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies at Columbia University. He is a member of the Science and Security Board of the Bulletin of Atomic Scientists, and an elected fellow of the American Association for the Advancement of Science (AAAS). He holds a doctorate in physics from MIT.

2.1 The Information Function

Until 2018, US joint military doctrine recognized six joint functions that were common to operations at all levels of warfare: command and control, intelligence, fires, movement and maneuver, protection, and sustainment. In October 2018, Joint Publication (JP) 3-0 (2017 Incorporating Change 1 from 2018) added the information function.[4]

Under JP 3-0 (2017 Incorporating Change 1 from 2018), the information function manages and uses information to change or maintain elements such as perceptions and attitudes to influence desired behaviors and to support human and automated decision-making. Importantly, this publication emphasizes that all military activities produce information, which in turn affects the perceptions and attitudes that drive behavior and decision-making.

The information function includes three sets of activities. The first is understanding information in the operational environment, i.e., the perceptions, attitudes, and decision-making processes of relevant actors informed by an appreciation of their culture, history, and narratives, as well as knowledge of the means, context, and established patterns of their communication.

The second set of activities involves leveraging information to influence the behavior of relevant actors through their perceptions, attitudes, and other drivers; to accurately inform domestic and international audiences to put operations into context and to facilitate informed perceptions about military operations; to counter adversarial misinformation, disinformation, and propaganda; and to attack, exploit, and cast doubt on non-friendly information, information networks, and systems to gain military advantage.

The third set of activities is support of friendly human and automated decision-making, i.e., facilitating shared understanding across the entire force and protecting friendly information, information networks, and systems.

JP 3-0 (2017 Incorporating Change 1 from 2018) notes that information (and C2 and intelligence) apply to all military operations, while the other joint functions may or may not apply depending on the purpose of the operations in question. It calls upon the commander to plan all operations so as to influence relevant actors and to benefit from the inherent informational aspects of physical power, but it takes special note of certain means with which to leverage information: key leader engagement; public affairs; civil-military operations; military deception; military information support operations; operations security; electronic warfare; space operations; special technical operations; and cyberspace operations. As it happens, these means are also key elements of JP 3-13 *Information Operations* (JP 3-13 (2012)) (see Section 2.3 below).

2.2 Information Warfare

Within the DoD, the term “information warfare” was apparently introduced Department-wide in a then-classified DoD Directive dated December 1992 with that term as its subject.[5] This directive defined “information warfare” as “[t]he competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information systems through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information systems from such attacks."

However, possibly limited by classification, this view of information warfare did not become part of joint doctrine until 1996 with the publication of JP 3-13.1 *Joint Doctrine for Command and Control Warfare.*[6] This document defined "information warfare" as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."

In 1998, DoD changed the definition of "information warfare" in JP 3-13 *Joint Doctrine for Information Operations* (JP 3-13 (1998))[7] to mean "IO [information operations] conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries." This publication also defined "information operations" as "actions taken to affect adversary information and information systems while defending one's own information and information systems." This definition of information warfare is virtually identical in content to what DoD understands today as cyberspace operations, as discussed in Section 2.6. Of particular importance is the fact noted in that section that cyberspace operations (often called cyber operations) are generally understood to involve access to and manipulations of computing or communications technology (both hardware and software).

2.3 Information Operations

The 2006 version of JP 3-13 *Information Operations* (JP 3-13 (2006)) replaced the term "information warfare" with "information operations,"[8] which it defined to include electronic warfare, psychological operations, military deception, and operations security in addition to computer network operations.[9] The terms added to the definition of information operations were previously part of what DoD had called "command and control warfare" in JP 3-13.1, *Joint Doctrine for Command and Control Warfare*.[10] Furthermore, JP 3-13 (2006) expanded information operations to include influencing, disrupting, corrupting, or usurping adversarial human, as well as automated-decision-making while protecting US decision-making.[11]

JP 3-13 (2006) also introduced the concept of the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information," noting that "the information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision-making." This information environment includes a physical dimension (i.e., the entities that enable individuals and organizations to create effects), an informational dimension (where and how information is collected, processed, stored, disseminated, and protected), and a cognitive dimension (i.e., the minds of those who transmit, receive, and respond to or act on information). Yet the information environment construct did not play a central role in JP 3-13 (2006).

In 2012, DoD issued JP3-13 *Information Operations* (JP3-13 (2012)),[12] which changed the 2006 version in three significant ways. First, it elevated the importance of the information environment since information-related capabilities (IRCs) are defined in terms of their ability to affect the information environment. Second, it changed the focus of information operations from a list of operations to "the integrated employment, during military operations, of IRCs 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." Third, JP 3-13 (2012) emphasized that information operations are not about ownership of individual capabilities (hence the elimination of the list of activities that constitute information operations) but rather the use of those capabilities to create a desired effect.

More formally, JP 3-13 (2012) defined IRCs as the tools, techniques, or activities that affect the information environment. It also identifies a larger number of capabilities that contribute to information operations: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations, information assurance, space operations, military information support operations (formerly psychological operations, or PSYOP), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations (colloquially known as electronic warfare), and key leader engagement. Further, within the constructs of JP 3-13 (2012), cyberspace is recognized to be wholly contained within the information environment—the logical implication being that cyberspace operations necessarily affect the information environment and furthermore that cyberspace operations are, in fact, an information-related capability.

In 2014, the DoD issued JP 3-13 (2012 Incorporating Change1 from 2014).[13] Differing from the 2012 version only in its addition of doctrine related to the assessment of information operations, JP 3-13 (2012 Incorporating Change1 from 2014) predates JP 3-0 (2017 Incorporating Change 1 from 2018) by several years. Thus, it would not be surprising to see the next version of JP3-13 to track the discussion of the information function more closely in JP 3-0.

2.4 Influence Operations

The term "influence operations" appears to have no DoD (or U.S. Government) definition. Yet the 2009 RAND study *Foundations of Effective Influence Operations* defines influence operations as the "application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further US interests and objectives."[14] This study also noted specifically that although influence operations usually emphasize communications to affect attitudes and behaviors, they can also use military capabilities, economic development, and other in-real-life capabilities to reinforce these communications. RAND views are not necessarily authoritative, but RAND has been a primary analytical resource for the Department of Defense, though an independent one, for many decades.

2.5 Psychological Operations

Psychological operations are a key component of information operations, and the NPR and WP stories both refer to them. JP 3-13.2, *Psychological Operations* (JP 3-13.2 (2010))[15] and its follow-on JP 3-13.2 *Military Information Support Operations* (JP 3-13.2 2010 Incorporating Change 1, December 20, 2011)[16] define psychological operations (or military information support operations as they are now known in DoD's lexicon) as the conveyance of "selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives." These doctrinal documents also indicate that "it is important not to confuse psychological impact with PSYOP. Actions of the joint force, such as strikes or shows of force have psychological impact but they are not PSYOP unless their primary purpose is to influence the perceptions and subsequent behavior of a TA [target audience]."[17] Note also that the definition does not restrict psychological operations to conveying truthful information. For practical or operational reasons (such as the damage to US objectives that might result should lies be discovered), it may be wise to restrict a psychological operation to conveying truthful information, but nothing in the definition requires it.

JP 3-13.2 contains two curious omissions. First, it does not include counterpropaganda activities, which are understood to be activities that identify adversary propaganda (defined as communication designed to influence the opinions, emotions, attitudes, or behavior of any group to benefit the adversary), contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. This definition of counterpropaganda was present in JP 3-53, *Doctrine for Joint Psychological Operations* (2003), the predecessor of JP 3-13.2; the term was also eliminated from JP 1-02 DOD Dictionary and Associated Terms in the 2010 version.

Second, the DoD definition of psychological operations in JP 3-13.2 does not explicitly acknowledge the possibility that US audiences (or armed forces) could be the target of adversary psychological operations to influence the emotions, motives, objective reasoning, and ultimately the behavior of US actors—definitions of other DoD operations do incorporate the idea that US forces conduct operations to compromise adversary functions while protecting those same for US forces. It is possible that this omission is directly or indirectly a result of DoD policy: DoD Directive 3600.01 *Information Operations* states explicitly that "DoD IO activities will not be directed at or intended to manipulate audiences, public actions, or opinions in the United States and will be conducted in accordance with all applicable US statutes, codes, and laws,"[18] and activities that seek to counter adversary psychological operations could be construed as violating this directive.

2.6 Cyberspace Operations

JP 3-12(R) *Cyberspace Operations* was first introduced in 2013,[19] and a second revised version published in 2018.[20] Both versions define a cyberspace capability as "a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace," and cyberspace operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Note in particular the technical focus of cyberspace operations.[21]

JP 3-12 (2018) states that all cyberspace operations are part of one of three cyberspace missions: DoD Information Network (DODIN) operations, defensive cyberspace operations, or offensive cyberspace operations. DODIN operations secure, configure, operate, extend, maintain, and continuously sustain on an ongoing basis DoD cyberspace, and create and preserve the confidentiality, availability, and integrity of the DODIN. Defensive cyberspace operations defend the DODIN from specific threats that have bypassed, breached, or are threatening to breach DODIN security measures, and defend other cyberspace assets that the DoD has been specifically ordered to defend. Offensive cyberspace operations project power in and through foreign cyberspace. They may exclusively target adversary cyberspace functions, or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, and so on.

JP 3-12 (2018) also describes how cyberspace operations contribute to the joint functions of command and control, intelligence, fires, movement and maneuver, protection, sustainment, and, most importantly, information. After repeating the discussion of the information function contained in JP 3-0 (2017 Incorporating Change 1 from 2008), JP 3-12 (2018) describes cyberspace as a medium through which specific information capabilities, such as military information support operations or military deception, may be employed. It notes that while some operations in the information environment may be done using only cyberspace operations, other such operations may not involve them.

3. INFORMATION AND CULTURAL DYSFUNCTION IN DOD

It is important to consider the information function itself in relation to the other joint functions. As noted in Section 2.1, JP3-0 (2017 Incorporating Change 1 from 2018) added information as a joint function essential to military operations at all levels of warfare. These other functions are:

- Command and control, which encompasses the commander's exercise of authority and direction over assigned and attached forces to accomplish the mission,[22]
- Intelligence, which informs commanders about adversary capabilities, centers of gravity, vulnerabilities, and future courses of actions, and helps commanders and staffs understand and map friendly, neutral, and threat networks,[23]
- Directing fires of available weapons and other systems, which creates a specific effect on target(s), both destructive and non-destructive,[24]

- Movement and maneuver secure positional advantages before or during combat operations,[25] and
- Protection, which helps preserve the fighting potential of the commander's forces.[26]
- Sustainment, which entails logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force.[27]

These seven functions are described as essential to all military operations, yet the fact that previous versions of JP 3-0 did not explicitly include information suggests that DoD did not view information to be as important as the others. According to one account provided by a senior military cyber commander,[28] the doctrinal authorities recognized that adversaries were accomplishing goals in the operational environment (in which the original six functions resided) solely through activities in the information environment. Adoption of the information function was their way of reconciling the growing importance of information-centric activities with the operational environment and the primacy of the first six functions at the center of previous doctrinal formulations.

As noted in Section 2.1, the description in JP3-0 (2017 Incorporating Change 1 from 2018) of the information function calls for the commander to plan all operations to influence relevant actors and to benefit from the inherent informational aspects of physical power. C2, intelligence, and information are functions that apply to all military operations, but of these three, only information is outwardly relevant—that is, it seeks to influence non-US actors. Furthermore, JP 3-0 (2017 Incorporating Change 1 from 2018) notes that the other joint functions may be necessary only in some other military operations, depending on their scope and goals.

Put differently, information is the only function that is both outwardly as well as inwardly directed and is applicable to all military operations. As the information environment is increasingly overlaid on top of the operational environment, information will be uniquely and increasingly importantly cross-cutting among the joint functions. On the other hand, and despite rhetoric and doctrinal statements to the contrary, US military culture is oriented towards the physical world and the operational environment. It has historically looked to the operational environment as where battles are won, and mass, firepower, and technological overmatch have been regarded as the tools with which to win battles, and physical engagement, courage, and bravery are honored above other personal attributes in soldiers. The patron saint of US military culture writ large is much more Clausewitz, who emphasizes the need to destroy the enemy's means of physical resistance,[29] than Sun Tzu, who emphasizes the desirability of winning without fighting.[30]

This ethos surfaced conspicuously in February 2013 with the proposed Distinguished Warfare Medal (DWM), introduced by then-Secretary of Defense (SECDEF) Leon Panetta to provide "distinct, department-wide recognition for the extraordinary achievements that directly impact on combat operations, but that do not involve acts of valor or physical risk that combat entails."[31] By design and intent, this medal was to be awarded not for acts of battlefield valor, but rather, for key contributions to combat operations whether or not within a combat zone. DoD provided two examples of medal worthy acts: a Nevada-based operator of a remotely piloted vehicle flying in Afghanistan, and a Fort Meade-based Soldier who detects and thwarts a cyberattack on a DOD computer system. This medal would have ranked above the Purple Heart and Bronze Star, and below the Distinguished Flying Cross.

Despite DoD's resolve to avoid having this new medal detract from valor decorations, (e.g., the Medal of Honor, Service Crosses, and Silver Star Medals), serious controversy arose for that very reason. Critics all acknowledged the need to recognize those who contribute significantly to combat operations, but hotly disputed placing the DWM above the Purple Heart and decorations that honor physical bravery. For example, one critic said, "Medals that can only be earned in direct combat must mean more than medals awarded in the rear.[32] Another stated that "to rank what is basically an award for meritorious service higher than any award for heroism is degrading and insulting to every American Combat Soldier, Airman, Sailor or Marine who risks his or her life and endures the daily rigors of combat in a hostile environment."[33] Two months later the DWM was canceled by the incoming SECDEF, Chuck Hagel.

The sentiment underlying such comments is clear—one's physical bravery is prized over and above the value of one's contribution to the achievement of US military goals. It is thus not entirely surprising that some do not view soldiers with non-kinetic specialties with the same respect as they do for combat arms troops with specializations in more traditional fields such as infantry, armor, and artillery. Indeed, soldiers specializing in information operations—and especially psychological operations—often report feeling that others regard them with disdain and contempt.

A similar mindset can be found in the debate over physical fitness requirements for cyber soldiers. Several things are unassailable in this debate. First, the ability to "fight" on the cyber battlefield is not highly correlated with one's physical fitness. Second, the actual conduct of cyber operations can be largely though not exclusively conducted remotely from areas in which physical attributes are again not particularly valuable. Third, higher standards for physical fitness will inevitably result in a smaller pool of those with the skill sets needed for the cyber battlefield. And yet, when the services continue to resist these realities, they degrade their own cyber capabilities—a very clear sign that these capabilities are not as highly valued as other capabilities relevant to military engagement.

Psychological operations have also been singled out for some negative comparisons even among the non-kinetic combat capabilities. In 2011, the term "psychological operations" (PSYOP) was superseded by "military information support operations," on the directive of then-SECDEF Robert Gates, whose explanation for the name change was that "although psyop activities rely on truthful information, credibly conveyed, the term PSYOP tends to connote propaganda, brainwashing, manipulation, and deceit."[34] Indeed, JP 3-13-2 *Military Information*

Support Operations, explains that such operations “create and reinforce actions that are executed to deliberately mislead adversary military decision makers about US military capabilities, intentions, and operations.”

The conduct of psychological operations also tends to require higher authorities than for kinetic operations. For example, during Operation INHERENT RESOLVE, the authority to strike ISIS kinetically required a brigadier general or even below, while an information operation—including a psychological or military information support operation—required the approval of a at least a major general. Indeed, at the start of Operation INHERENT RESOLVE, some such operations required approval at the level of the National Security Council (NSC). Any such operation conducted via the Internet or social media required Pentagon-level approval.[35] These constraints have led some to wryly conclude that “it is easier to get permission to kill terrorists than it is to lie to them.”

Organizationally, Army psychological operations personnel constitute most of DoD psychological operations personnel. Most of these Army personnel are under the operational command of the Army Public Affairs and Psychological Operations Command,[36] which itself is an Army Reserve command. Only a relatively small fraction of Army psychological operations personnel are active-duty soldiers under the operational command of U.S. Special Operations Command (USSOCOM).

At the level of the U.S. Government, Carnes Lord takes note of American cultural inhibitions with respect to psychological operations,[37] pointing to a tendency to “discount the relevance of nonmaterial factors such as history, culture and ideas . . . [and] to assume that concrete interests such as economic well-being, personal freedom, and security of life and limb are the critical determinants of political behavior everywhere, the extreme difficulty of “Americans [in dealing] effectively in international settings where basic American values are under challenge”, a manifest or latent “distaste for any sort of psychological manipulation or deception,” and an idea that psychological operations are “a black art that can be morally justified only under the most extreme circumstances.”

DoD policy also forbids information operations that manipulate audiences, public actions, or opinions in the US. As a result of that policy, DoD cannot directly take actions to mitigate the effects of adversary information-based campaigns against US citizens—it can only act against those responsible for conducting such campaigns, even though as described in Section 2.5 it once had considerable counterpropaganda knowledge and expertise that would be relevant to such a goal.

Tasking DoD to conduct direct defensive operations to protect Americans against foreign influence is beyond the scope of this article, and arguably a bad idea—perhaps even Constitutionally suspect as well. But under existing law,[38] DoD can support civilian authorities (e.g., it can help prepare, prevent, protect, respond, and recover from domestic incidents). Thus, DoD cannot act in a counter-propaganda role to protect US citizens from malign foreign influence, but it can lend expertise and knowledge to civilian authorities, such as the Department of Homeland Security (DHS) or state and local governments, as requested.

4. DISCUSSION

The previous sections highlight some of the ambiguity in public discussions mentioned in Section 1. Cyber operators performing in offensive cyberspace operations are providing fires, yet an offensive cyber operation also can serve to materially impact the decision-making processes of an adversary. When the goal of an offensive cyber operation is to affect adversary decision-making processes, that operation can be regarded as an information operation, specifically a psychological operation.

At the same time, the doctrinal history holds an important lesson for internal DoD discourse about information warfare, information operations, and the like, and communicating with the US public about such topics. Outside the DoD specialist community, the terms "information operations" and "information warfare" have evolved to be more or less synonymous with the deliberate spread of disinformation for adversarial purposes; that is, they are more limited in scope than DoD usage conventions. This is true outside the DoD as well.[39] This common understanding of information operations and information warfare is quite similar to DoD's definition of psychological operations as described in Section 2.5.

Such conflations are not new. In a May 2007 article,[40] Curtis Boyd (then assistant chief of staff, G3, at the U.S. Army Civil Affairs and Psychological Operations Command) pointed to the widespread adoption of "information operations" as a euphemism for psychological operations. He observed that "unified combatant command theater security cooperation plans . . . routinely use[d] IO synonymously for PSYOP to describe regional security information programs, activities, and exercises with other nations. . ." Further he noted several examples of such conflation: a retired major general who wrote that he used IO and PSYOP interchangeably in describing activities in Bosnia; then-SECDEF Donald Rumsfeld describing leaflet drops and Commando Solo broadcasts (typically activities conducted by psychological operations personnel) as IO preparation weapons against Iraq; and the description of a Marine Corps platoon leader of Iraqi troops surrendering as the result of an intense "information operations" campaign that dropped leaflets and broadcasted surrender appeals from loudspeakers.

Although the Boyd article was published in 2007, there is little evidence that such usage has changed in the interim. Indeed, *The Washington Post* article cited above uses the term "information warfare" as being generally synonymous with the activities being conducted, presumably based on interactions with knowledgeable DoD personnel. Apparently, the term "information warfare" is often used to refer to a state-on-state use of cyber-enabled propaganda campaigns aimed at national publics, which is an even more restricted formulation with no obvious analog within the DoD lexicon. It may be true that cyberspace operations as understood within DoD doctrine can be used to deliver psychological effects, but the understanding in common parlance is that cyberspace operations affect silicon-based machines and psychological operations (as well as information operations, influence operations, and information warfare) that affect human minds.

To sum up, I am suggesting that the history and evolution of doctrinal constructs in these domains have led to a situation in which non-cyber and non-MISO DoD personnel view terms and concepts such as information warfare and information operations more similarly to how these terms are used in societal discourse than to how cyber and MISO specialists understand them.[41] Using these same terms differently in different contexts is likely to create conceptual confusion that in turn can also result in misallocation and misalignment of resources and capabilities.

For example, such confusion may make it more difficult to recruit, hire and train the right people due to a lack of understanding about what different missions and skill sets actually entail. If recruiters are unable to clearly articulate what missions entail, they will be unable to hire people whose qualifications are optimized to perform those missions. Similar concerns attach to performance evaluation—without a clear articulation of what effective mission performance means, it is more difficult to differentiate between high and low performers.

Perhaps of greatest significance are the cultural considerations discussed in Section 3 as they potentially affect doctrinal formulations. As that section pointed out, non-kinetic military specializations are not as highly ranked in the DoD cultural hierarchy (aka the pecking order) as kinetic specializations, and it would not be surprising if the lack of respect accorded the former translated into a lack of significant attention to such matters on the part of the latter. Everyone is busy, and for matters deemed of lesser importance, incentives to familiarize oneself with such matters are likely to be scarce.

The comments above reflect a degree of cultural dysfunction within DoD regarding information operations (contrasted with kinetic operations) and more so for psychological operations. Overall, they suggest that the full incorporation of psychological operations into military operations will continue to face an uphill battle within the DoD community.

5. CONCLUSION

The *Army Times* reported in late 2019 that U.S. Army Cyber Command (ARCYBER) was proposing to change its name to Army Information Warfare Command,[42] quoting Lt. Gen. Stephen Fogarty, Commander, ARCYBER, as saying “Sometimes, the best thing I can do on the cyber side is actually to deliver content, deliver a message. ... Maybe the cyberspace operation I’m going to conduct actually creates some type of [information operation] effect.”

Assuming this is an accurate quote, a careful parsing of words suggests that Lt. Gen. Fogarty’s words are consistent with the comments of Section 4—cyberspace operations are being used to deliver a psychological effect. These words also coincide with guidance in JP 3-13.2, *Military Information Support Operations*: "Computer network operations [approximately equivalent to today's cyberspace operations] support MIS [military information support] forces with dissemination assets (including interactive Internet activities) and the capabilities to deny or degrade an adversary's ability to access, report, process, or disseminate information."

A name change to Army Information Warfare Command would expand the 1998 definition of information warfare, which Section 2.2 pointed out was essentially synonymous with what are known today as cyberspace operations. Everything that falls within the full scope of the expanded definition of information warfare is unknown (at least to me), but at a minimum, it seems to include psychological operations (or MISO) as well as cyberspace operations.

A similar story appears to be true of the Air Force. The 16th Air Force, known as Air Forces Cyber and the Air Force's Information Warfare Numbered Air Force integrates multisource intelligence, surveillance, and reconnaissance, cyber warfare, electronic warfare, and information operations capabilities across the conflict continuum.[43] Prior to its creation in October 2019, one press report quoted a senior Air Force official as saying that "We've come to discover cyber is an element of the larger information warfare and [electromagnetic spectrum] fight that we're in," and that "to view cyber in its lane and in the functional stovepipe is really an incomplete analysis. We've come to discover it's really information warfare."[44] The same article reported him as saying that the new organization [that is, the organization that would become the 16th Air Force] will focus on "cyber information operations, influence operations, electronic warfare, military deception, military information support operations and psychological operations."

However, in late February 2020, a search of the 16th Air Force web site for "military information support operations" turned up zero references. The word "psychological" yielded one reference—a reference to a component of 16th Air Force (the 480th ISR Wing) that conducted psychological operations in 1952 and was subsequently deactivated in 1953. The site contains many references to "information operations," but examination of these references suggests no connection to psychological operations or military information support operations. The site is also replete with references to "cyber," and the commander of the 16th Air Force has a background that is squarely in the cyber domain as the commander of the cyber National Mission Force.

The strongly technical emphasis and history of the DoD cyber warfare community cause me to question whether DoD is well-positioned to embrace and integrate the psychological aspects of information operations.[45] Various service cyber commands (including USCYBERCOM) have concentrated on acquiring the technical expertise that cyberspace operations require. This focus has been entirely proper given their missions to date, but the expertise needed to conduct psychological operations goes beyond the skill set of cyber operators. Nor do the various cyber commands appear particularly interested in obtaining such expertise—a keyword search on USAJOBS (conducted in late February 2020) for jobs involving "cyber" and "psychology" or "cyber" and "psychological" turned up nothing, and of 44 jobs listings resulting from a keyword search on “cyber command,” exactly zero jobs entailed anything remotely connected to psychology.

The DoD needs a standing operational entity that can integrate specialists in psychological operations and in cyber operations as co-equal partners. As my *Lawfare* posting indicated, “bringing to bear the respective expertise of each command [Cyber Command for cyber expertise, Special Operations Command [USSOCOM] for psychological operations] should . . . enhance the synergies possible between cyber-enabled psychological operations and offensive cyber operations, and it would be most desirable if the two commands could partner rather than compete over the cyber-enabled psychological operations mission.”

The “standing” part of this entity (or entities) is essential, as it would recognize the continuing need to conduct such operations against adversaries who believe that open conflict need not have been declared or even started for hostile activity in information space to begin. To cite just one example, former Russian Deputy Chief of the General Staff Lt-Gen Aleksandr Burutin noted in January 2008 that information weapons can be “used in an efficient manner in peacetime as well as during war.”[46] Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), pointed out that “the Russians use information from a covert stage through six phases of warfare to the re-establishment of victory. Information confrontation is conducted in every phase, including covertly, in peace and in war.”[47]

Many military missions today are conducted under the auspices of joint task forces assembled specifically to conduct individual missions. Although these missions generally have well-defined start and end points, there is precedent for standing joint task forces. In particular, a series of joint task forces were established in the late 1990s to deal with the challenges of defending US information assets and projecting power in cyberspace. Joint Task Force-Computer Network Defense (JTF-CND) attained initial operating capability in December 1998 and reported directly to the Secretary of Defense. JTF-CND evolved into Joint Task Force – Computer Network Operations (JTF-CNO) by the end of 1999, and JTF-CNO itself turned into Joint Task Force on Global Network Operations (JTF-GNO) in 2004.[48] This history is noteworthy for the similarity of the cyberspace mission set to that of military information support operations—adversaries pose ongoing and continuing challenges both in cyberspace and in human “brain space, and addressing such challenges is a mission that never ends.

A lighter-weight alternative to a standing JTF could call for similarly structured functional components integrated into the geographical commands. As functional components, they would integrate cyber and PSYOP capabilities. As elements of geographical commands, they would be directly responsive to the needs of theater commanders, reducing the likelihood of deconfliction issues arising from the activities of an entity outside the purview of those commanders. The regional expertise needed for effective psychological operations would also be more readily available with integration into geographical commands. And there is precedent for functional components of combatant commands—in 2005, U.S. Strategic Command (USSTRATCOM) established the Joint Functional Combatant Command for Network Warfare.[49]

I am personally agnostic on the specific form of this operational entity, as long as it meets the two requirements of functional integration and permanence. Whether the right construct is a standing Joint Task Force for Cyber-Enabled Military Information Support Operations reporting to the Secretary of Defense, theater-based joint functional combatant commands for cyber-enabled military information support operations, or something else, the DoD needs to move forward organizationally if it is to have any hope of getting ahead of this new form of warfare.

ACKNOWLEDGEMENTS

Pablo Breuer, Edward Cardon, Jessica Dawson, Matt Ellison, Karen Guttieri, Joseph Reeder, Robert Ross, Jennifer Snow, William Spracher, and Michael Warner offered valuable feedback on initial drafts of this paper. I am to blame for any errors in this paper.

NOTES

1. Herb Lin, "On the Integration of Psychological Operations with Cyber Operations," *Lawfare* (blog), January 9, 2020, https://www.lawfareblog.com/integration-psychological-operations-cyber-operations.
2. Dina Temple-Raston, "How The U.S. Hacked ISIS," *NPR.Org*, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.
3 . Ellen Nakashima, "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election," Washington Post, December 25, 2019, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.
4. Joint Chiefs of Staff, Joint Publication 3-0 *Joint Operations (2017 Incorporating Change 1 from 2018)*, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.
5. Donald J. Atwood, Deputy Secretary of Defense, "Information Warfare," Department of Defense Directive (DoDD) TS 3600.1), December 21, 1992. A redacted version of this document can be found at http://www.dod.mil/pubs/foi/Reading_Room/Other/14-F-0492_doc_01_Directive_TS-3600-1.pdf. Cited in Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014," Cyber Defense Review (online version), August 27, 2015, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.
6. Joint Chiefs of Staff, "Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)" (Washington D.C., February 7, 1996), http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf.
7. Joint Chiefs of Staff, "Joint Publication 3-13: Joint Doctrine for Information Operations" (Washington D.C., October 9, 1998), http://www.c4i.org/jp3_13.pdf.
8. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations" (Washington D.C., February 13, 2006), https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf.
9. Michael Warner, US Cyber Command historian, has noted that the phrase "information operations" first replaced the term "information warfare" in the DOD lexicon as the result of then-classified DOD directive (DoDD S-3600.1), even though the actual definition of the term remained the same. See Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014," Cyber Defense Review (online version), August 27, 2015, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.
10. Joint Chiefs of Staff, "Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)" (Washington D.C., February 7, 1996), http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf.
11. JP3-13, Information Operations, (2006), I-1.
12. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations" (Washington D.C., November 27, 2012), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf.
13. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations" (Washington D.C., November 20, 2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.
14. Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.
15. Joint Chiefs of Staff, "Joint Publication 3-13.2: Psychological Operations" (Washington D.C., January 7, 2010), https://fas.org/irp/doddir/dod/jp3-13-2.pdf.
16. Joint Chiefs of Staff, "Joint Publication 3-13.2: Military Information Support Operations" (Washington D.C., December 20, 2011), https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf.
17. JP3-13.2, Psychological Operations, I-1.
18. DOD Directive 3600.01 Information Operations , USD Policy, May 2, 2013 Incorporating Change 1, May 4, 2017 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf
19. Joint Chiefs of Staff, "Joint Publication 3-12 (R): Cyberspace Operations" (Washington D.C., February 5, 2013), https://fas.org/irp/doddir/dod/jp3_12r.pdf.
20. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations" (Washington D.C., June 8, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

NOTES

21. Note also that the U.S. government as a whole defines cybersecurity as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." (See NSPD-54, available at https://fas.org/irp/offdocs/nspd/nspd-54.pdf.). Here the technology-centric connotations of the term "cybersecurity" are readily apparent.
22. JP3-0 (2017 Incorporating Change 1 from 2018), III-2.
23. JP3-0 (2017 Incorporating Change 1 from 2018), III-27.
24. JP3-0 (2017 Incorporating Change 1 from 2018), III-30.
25. JP3-0 (2017 Incorporating Change 1 from 2018), III-37.
26. JP3-0 (2017 Incorporating Change 1 from 2018), III-39.
27. JP3-0 (2017 Incorporating Change 1 from 2018), III-47.
28. Lt. Gen. (Ret.) Edward C. Cardon, former Commanding General of U.S. Army Cyber Command (2013-2016), personal communication, February 20, 2020.
29. For example, Clausewitz writes that "Direct annihilation of the enemy's forces must always be the dominant consideration," (p 228) as "destruction of the enemy's forces is the overriding principle of war." (p 258), Carl von Clausewitz, On War, edited and translated by Michael Eliot Howard and Peter Paret, Princeton University Press, 1976, https://press.princeton.edu/books/paperback/9780691018546/on-war.
30. For example, Sun Tzu writes that "to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.". From Sun Tzu, The Art of War, Samuel B. Griffith (tr.), Oxford University Press (1963), 76.
31. Jim Garamone, "Panetta Announces Distinguished Warfare Medal," *American Forces Press Sources*, February 13, 2018, https://archive.defense.gov/news/newsarticle.aspx?id=119290.
32. "VFW Wants New Medal Ranking Lowered," VFW: Veterans of Foreign Wars, February 14, 2013, https://www.vfw.org/media-and-events/latest-releases/archives/2013/2/vfw-wants-new-medal-ranking-lowered.
33. "Military Order of the Purple Heart," Military Order of the Purple Heart, February 15, 2013, https://web.archive.org/web/20180621131408/http:/www.purpleheart.org:80/News.aspx?Identity=238.
34. U.S. Marine Corps, "Changing The Term Psychological Operations to Military Information Support Operations" (Washington D.C.: U.S. Marine Corps, December 12, 2011), https://www.marines.mil/News/Messages/MARADMINS/Article/887791/changing-the-term-psychological-operations-to-military-information-support-oper/.
35. Cole Livieratos, "Bombs, Not Broadcasts", *Joint Forces Quarterly*, Number 90, 3rd Quarter 2018, 60-67, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90.pdf.
36. "About Us: U.S. Army Civil Affairs & Psychological Operations Command (Airborne)" (Fort Bragg, NC: U.S. Army Reserve), https://www.usar.army.mil/Commands/Functional/USACAPOC/About-Us/.
37. Carnes Lord, "The Psychological Dimension in National Strategy," in Frank Goldstein and Benjamin Findley (eds.), *Psychological Operations: Principles and Case Studies*, Air University Press, 1996, 73-89, https://media.defense.gov/2017/Apr/07/2001728209/-1/-1/0/B_0018_GOLDSTEIN_FINDLEY_PSYCHLOGICAL_OPERATIONS.PDF.
38. Joint Chiefs of Staff, "Joint Publication 3-28, *Defense Support to Civilian Authorities,"* Washington D.C., October 29, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.
39. For example, Facebook defines information operations as "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome," possibly using "a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion." Jen Weedon, William Nuland and Alex Stamos, Information Operations and Facebook, Version 1.0, Facebook, April 27, 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.
40. Curtis Boyd, "Army IO is PSYOP Influencing More with Less," Military Review 87(3): May-June 2007, 67-75, https://apps.dtic.mil/dtic/tr/fulltext/u2/a575201.pdf.

NOTES

41. Christopher Paul reached a similar conclusion in March 2019 on a RAND blog, and one element of his preferred way forward is simply to abandon the term "information operations." See Christopher Paul, "Is It Time to Abandon the Term Information Operations?," March 13, 2019, https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html.
42. Kyle Rempfer, "Army Cyber Lobbies for Name Change This Year, as Information Warfare Grows in Importance," *Army Times*, October 16, 2019, https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/.
43. "Fact Sheet: Sixteenth Air Force (Air Forces Cyber)," October 18, 2019, https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/.
44. Mark Pomerleau, "Air Force Hopes New Organization Can Boost Electronic Warfare," *C4ISRNET*, April 15, 2019, https://www.c4isrnet.com/electronic-warfare/2019/04/15/air-force-hopes-new-organization-can-boost-electronic-warfare/.
45. The discussion here focuses on the psychological aspects. The same may well be true for other facets of information operations.
46. Interfax-AVN news agency, January 31, 2008.
47. "Russia: Implications for UK defence and security," First Report of Session 2016–17, House of Commons Defence Committee, UK Parliament, July 5, 2016, 17.
48. "Command History," U.S. Cyber Command, https://www.cybercom.mil/About/History/.

49 *op cit*. "Command History," U.S. Cyber Command.