ARTICLE

Dealing with Disinformation:

The Barriers to Success and a Path Forward

James M. Davitch

In order to win in the information domain, the Department of Defense requires a new capability—an information fires team, engaged to combat disinformation. Working at the operational level, such a team will include military members skilled in global geopolitics, predictive analyses, metacognitive tools and theory, open-source information collection, and internal and external communication and messaging.

The US military's approach to information warfare relies on personnel, organizations, techniques, and procedures grounded in conventional doctrine.[1] When it comes to tactical information operations, instead of doing what the Joint force needs them to do, US military members do what they know how to do. This reality leaves combatant commanders at a comparative disadvantage relative to foes who use the information space to exploit a vulnerability of the United States while avoiding its historic conventional military strengths. Winning in the information domain today and tomorrow will require the Department of Defense to acquire a new capability. In conflicts with peer competitors, clear, concise, and correct communication is a major weapon of warfare.

This article advocates for a new kind of fires team to assist with this problem. The proposed "anti-disinformation" cell would compete in the cognitive rather than physical domain. The Department should begin to think about force packaging that includes not only traditional military hardware like ships, aircraft, and munitions, but also people who can help understand the geopolitical situation and communicate in a way advantageous for US national interests. Recommendations in this article are also pertinent to civilian national security leaders as they consider ways to respond to adversary moves and inform public opinion to help achieve political ends.

In a prescient 1997 essay, Richard Szafranski lays bare the consequences of falling behind adversaries who attempt to gain information advantages. When a citizenry's will, their country's technological edge, and that nation's claim to the moral high ground are in alignment, the pursuit of the profession of arms is useful and important. "If, however, the moral high ground is lost, a domino effect occurs: public support is lost, the technological high ground is lost, and the armed forces are lost."[2]

[1] I would like to thank Lieutenant General B. Chance Saltzman and Colonel Donald R. Brunk who helped clarify my thoughts through many valuable conversations. Additionally, I would like to thank the editorial team at Air University Press and two anonymous reviewers for their constructive comments on earlier versions of this article. All errors found herein are my own.

[2] Richard Szafranski, "A Theory of Information Warfare; Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995).

In the years since this warning, there has been no shortage of scholarship discussing the importance of information operations. Christopher Paul made an important argument in favor of information operations' outsized benefits relative to their cost.[3] Many articles have been published describing the need to think differently about the so-called information domain.[4] This article articulates the problems the military faces in the information domain, highlighting five barriers to success; presents a new force packaging concept focused an information fires team; and concludes by suggesting an implementation plan for senior leaders.

The Problem

The *Summary of the 2018 National Defense Strategy* highlights the need to address information warfare challenges because they test "our ability to deter aggression."[5] For the United States to effectively deter an adversary, it must first recognize what is happening and second, credibly warn the adversary of the negative consequences of its actions. Information warfare complicates deterrence because it injects confusion into perception and decision making.

The fog of war has always been a challenge. But the volume, variety, and velocity of information sources are growing at such a rate that the creation of new terms for the measurement of data (for example, exabytes, zettabytes, yottabytes) is increasing as rapidly as the data.[6] The confusion generated by the influx of data, much of it deceptively injected into the information domain, can slow US response times. This degrades the military's ability to credibly deter adversaries amid persistent, low-grade conflict. To compete, the military must reexamine how information warfare forces are organized and trained.

Information operations are not new, but they are nonetheless complex. The Joint Staff has enshrined information in doctrine, labeling it as the seventh Joint function.[7] As doctrine is the result of past experiences, this suggests the Defense Department has learned enough to be agile in its application. Yet across all levels of information operations, tensions persist between various interrelated elements—cognitive biases and

[3] Christopher Paul, "Enhancing US Efforts to Inform, Influence, and Persuade," *Parameters* 46, no. 3 (2016): 10.

[4] Will Atkins, Donghyung Cho, and Sean Yarroll, "More Cowbell: A Case Study in System Dynamics for Information Operations," *Air & Space Power Journal* 34, no. 2 (Summer 2020), https://www.airuniversity.af.edu/; US Joint Forces Command, *Commander's Handbook for Strategic Communication and Communication Strategy* (Suffolk, VA: Joint Warfighting Center, June 24, 2010), xiii; and, Justin Lynch, "Yet Another Article about Information Technology and the Character of War," War on the Rocks, September 2, 2020. https://warontherocks.com/.

[5] James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, January 2018), 3.

[6] Giuseppe Arbia, *Statistics, New Empiricism and Society in the Era of Big Data* (Cham, Switzerland: Springer, 2021).

[7] Chairman of the Joint Chiefs of Staff (CJCS), *Joint Concept for Integrated Campaigning* (Washington, DC: CJCS, March 16, 2018).

heuristics, training deficiencies, digital literacy limitations, security challenges, and epistemological hurdles. All five deserve scrutiny.

Information Warfare

Cognitive Challenges

In the information space, the advantage goes to the first mover, partially due to the cognitive biases psychologists call anchoring effects and framing effects. Both biases prey on the mind's tendency to be heavily influenced by the first piece of information heard and the proclivity to assume that information is true. In a combat environment, the rush to keep up with operations can result in a search for quick answers, and that tendency can cause more problems than it solves.

Confirmation bias, anchoring effects, and framing devices are especially hazardous for intelligence personnel who often encounter classified material as the first piece of information they examine and then endow it with outsized significance.[8] Worse still, the fixation on classified information can form barriers to creative thinking if it precludes the pursuit of additional, possibly contrary, forms of information. Searching for so-called disconfirming evidence is one of the techniques seasoned intelligence professionals employ as a counter to confirmation bias.[9] Unfortunately, classified information from exquisite sources often overshadows equally relevant but less exotic publicly available information that may contain disconfirming evidence.[10]

Training Challenges

Another reason why contending with information warfare is so difficult is due to the way military personnel are trained and educated for their jobs. Understanding how foes can manipulate social media has not historically been a prerequisite for military operations. This may be especially true in the Air Force, which prioritizes traditional science and technology undergraduate degrees. One consequence of this is that current Air Force personnel may be playing catch-up in a game that has already started. Analysis of nongovernmental Russian "digital mercenaries" found that successfully carrying out a disinformation campaign on social media platforms requires an understanding of platform affordances, audience segmentation and targeting strategies, and marketing best prac-

[8] Josh Kerbel, "The US Intelligence Community Wants Disruptive Change as Long as It's Not Disruptive," War on the Rocks, January 20, 2016, https://warontherocks.com/.

[9] *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 2009); and Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999).

[10] Anthony Olcott, *Open Source Intelligence in a Networked World* (New York: Continuum, 2012).

tices—skill sets not traditionally found within the state military and intelligence organizations most often responsible for information operations.[11]

Digital Literacy Challenges

Some argue the military needs to begin a crash program aimed at improving digital literacy.[12] But emerging scholarship shows there are differences between the ways military and civilian college students use social media that may put young officers at a disadvantage. Empirical research of student habits has shown a measurable gap between military academy, Reserve Officer Training Corps, and civilian student social media use.[13]

This data does not support a conclusion that military students are less capable at employing social media, but it does suggest cadets tend to use it less than civilians. This may result in a population of active-duty military personnel that are, at least initially, slightly less prepared to engage in tactics, techniques, and procedures for the application of "social media intelligence."[14]

Security Challenges

Another limitation the military faces is that personnel involved tend to operate without a shared understanding of what to discuss, if anything. In responding to adversary moves in the war for public opinion, sometimes personnel from as varied service backgrounds as intelligence, public affairs, legal, and foreign disclosure offices find themselves hastily assembled as information-warfare first responders. Through no fault of their own, individuals from these offices possess divergent viewpoints regarding releasing information to the public.

For some, such as intelligence personnel, information protection is a core job requirement. For public affairs professionals, information sharing is part of the daily routine. But all exist within a defense culture that tends to reward keeping rather than disclosing information. There is a good reason for this discretion: otherwise innocuous information can reveal, in sum, a larger picture of what the US government may be trying to hide.

Many military professionals today complete extensive information-protection training that encourages one to, when in doubt, protect data from being released. Clearly operational security is important, and the military still requires a degree of discretion when

[11] Renée DiResta, Shelby Grossman, and Alexandra Siegel, "In-House vs. Outsourced Trolls: How Digital Mercenaries Shape State Influence Strategies," *Political Communication* (published online December 2021), 3.

[12] Peter Singer and Eric Johnson, "The Need to Inoculate Military Servicemembers against Information Threats: The Case for Digital Literacy Training for the Force," War on the Rocks, February 1, 2021, https://warontherocks.com/.

[13] Karin K. De Angelis et al., "Ubiquity with a Dark Side: Civil-Military Gaps in Social Media Usage," in *Social Media and the Armed Forces*, ed. Eva Moehlecke de Baseggio, Olivia Schneider, and Tibor Szvircsev Tresch (Cham, Switzerland: Springer, 2020).

[14] David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security* 27, no. 6 (2012).

releasing some evidentiary material. But the demands of current operations require a military force with a different mindset. For example, current events unfolding between Russia and Ukraine are changing approaches to traditional information and security shibboleths. The Biden White House is demonstrating innovative ways of releasing selective pieces of information in an apparent attempt to combat disinformation while controlling the narrative during the crisis.[15]

Epistemological Challenges

The final complicating factor in information warfare relates to the pursuit of knowledge and divergent conceptions of truth, where truth is uncertain and elusive. This is not a new phenomenon. Thomas Rid traces a distinct upswing in information operations to the early Cold War years where two common understandings of truth emerged and hardened in opposition to each other.[16]

The first, analytical and apolitical truth, was based on shared norms and beliefs. Accordingly, the traditional intelligence process focused on the pursuit and acquisition of data in the hope that if enough data were acquired, truth will be found. To operate in this world, military personnel prepared for conventional force-on-force warfare in a sterile, positivist environment based on ostensibly objective facts and neat dichotomies of red forces opposite blue forces.[17]

This warfighting paradigm rewards deductive inferences and the acquisition of data. For instance, if one believes adversary forces are congregated at a certain location, aerial reconnaissance may be sent to observe it. Then a military commander may draw the conclusion that the adversary is or is not present. Imagery analysis can prove the fact that the adversary is there through physical, three-dimensional pictures. Of course, adversarial denial and deception techniques can obscure truth and cognitive factors such as the bias of the imagery analyst are still prevalent.

Still, a pervasive belief exists in military operations that the truth is objective and is supported by facts, data, and observation. In certain contexts, that is accurate. Yet in other contexts where truth is contested, that way of thinking is insufficient because there is also another truth.

Rid describes the second form of truth as ideological, emotional, and aligned with beliefs and values.[18] "The goal of disinformation is to engineer division by putting emotion over analysis."[19] The problem with expecting the military to compete in information warfare is

[15] Julian E. Barnes and Helene Cooper, "U.S. Battles Putin by Disclosing His Next Possible Move," *New York Times*, February 12, 2022, https://www.nytimes.com.

[16] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[17] Micah Zenko, "Millennium Challenge: The Real Story of a Corrupted Military Exercise and Its Legacy," War on the Rocks, November 5, 2015, https://warontherocks.com/.

[18] Rid, *Active Measures.*

[19] Rid, *Active Measures*, 426.

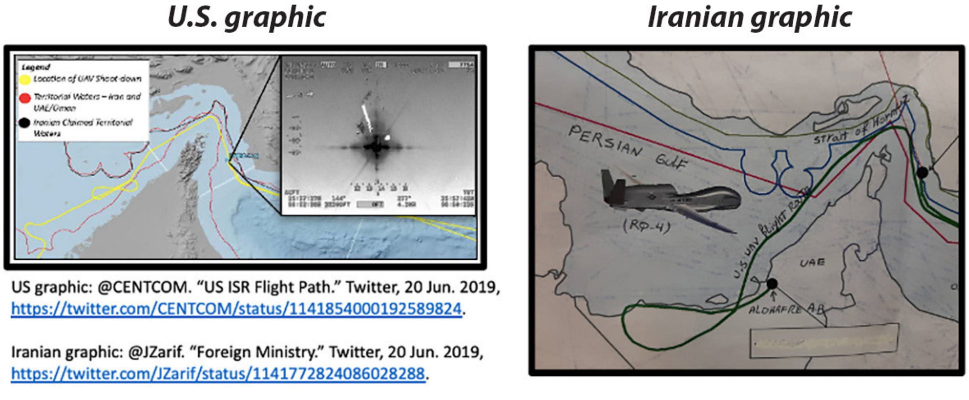
that conventional militaries train for and want to operate in an environment that puts analysis and facts over emotions and beliefs. In information operations, truth is constructed, context dependent, and relative based on an audience's preexisting belief structures.

Information operations must be more than accurate, they must be persuasive. This is because two understandings of truth exist, and while military personnel must be conversant in both to win militarily, maintain legitimacy, and retain public trust, most military members tend to be better at thinking in only one realm of truth.

Therefore, cognitive biases and challenges with training, digital literacy, security, and epistemology combine to create barriers to success in information warfare. The Department of Defense requires a new force-packaging concept that can overcome these obstacles. Combatant commanders need individuals who, in the information space, revel in the ambiguity of operations and can maneuver inside of the opponent's decision-making timeline. A team of individuals who can rapidly understand and contextualize the environment and communicate effectively to decision makers may form part of the solution.

Force Packaging

In June 2019, after Iran shot down a coalition unmanned aircraft in international waters, US Air Forces Central (AFCENT) responded to a conventional adversary with conventional weapons, including the F-22A Raptor's first deployment to Qatar. Iran followed the shootdown with a state-sponsored propaganda campaign designed to generate confusion and distrust of American intentions. A review of Iranian state-sponsored social media operations shows the goal of their information activities is to influence regional players' perceptions of the United States. Both Iran and America provided competing visual evidence for their arguments (fig. 1).[20]


U.S. graphic
Iranian graphic
Legend
● Location of UAV Shoot-down
● Territorial Waters – Iran and UAE/Oman
● Iranian Claimed Territorial Waters
PERSIAN GULF
Strait of Hormuz
(RQ-4)
U.S. UAV Flight Path
UAE
ALDHAFRE AB

US graphic: @CENTCOM. "US ISR Flight Path." Twitter, 20 Jun. 2019, https://twitter.com/CENTCOM/status/1141854000192589824.

Iranian graphic: @JZarif. "Foreign Ministry." Twitter, 20 Jun. 2019, https://twitter.com/JZarif/status/1141772824086028288.

Figure 1. US and Iranian graphics related to Iranian shootdown of unmanned aircraft in June 2019

[20] Seth G. Jones and Danika Newlee, *The United States' Soft War with Iran* (Washington DC: Center for Strategic and International Studies, 2019), https://www.csis.org/.

The speed with which US fighter jets, aircrew, and support personnel arrived to support US Central Command's F-22 request was impressive and demonstrated a key strength of the US Air Force to deploy conventional forces globally on short notice. But one lesson became clear in the weeks following the shootdown. United States information efforts did not adequately convince observers of Iranian intransigence.

Sensing this information failure, US Secretary of State Mike Pompeo accused the Iranian government of "sowing pure and blatant disinformation." He called the Iranian drawing "childlike" and concluded, "we need to make sure that every news outlet, everyone who is observing this, understands what's true and what the Iranian regime wants you to believe."[21] The United States was engaged in a fight for truth, something much less tangible than achieving airspace presence.

Recall that one of the primary objectives of disinformation is to privilege emotion over objective analysis. It is a weapon of the weak, especially for those adversaries that lack liberal democratic institutions. "For liberal democracies in particular, disinformation represents a double threat: being at the receiving end of active measures will undermine democratic institutions—and giving in to the temptation to design and deploy them will have the same result. It is impossible to excel at disinformation and democracy at the same time."[22] Therefore, it is time to think about the means of warfare as more than military equipment. Additionally, the Defense Department must consider how to employ counterdisinformation capabilities in accordance with core principles of liberal democratic governance.

The US Air Force excels at delivering supplies to coalition forces with mobility assets, finding adversaries with ISR sensors, and employing precision weapons. Yet warfighting requirements are changing with respect to new domains of competition. Military commanders should expand their inquiry beyond what traditional forces can be applied to an adversary. They must also ask what cognitive forces are needed to gain and maintain information advantages. The answers to such questions will allow leaders to manage the volatility of the Information Age, anticipate change, and predict upcoming challenges to military operations.[23]

On one hand, the loss of an unmanned aircraft due to a surface-to-air missile is a tactical issue best addressed in the way conventional forces have typically prepared for combat. At the same time, the strategic problem of the shootdown is how deliberate disinformation from an adversary can feed regional preexisting belief structures of US imperial overstretch. That narrative can play into the affective emotional response of regional Allies and partners. Further, it may have follow-on theater-wide ramifications beyond the initial aircraft loss that influence partners' decisions to allow access, basing, and overflight requests.

[21] Amanda Erickson, "Pompeo Accuses Iran of Spreading 'Blatant Misinformation' on Downing of Drone," *Washington Post*, June 23, 2019, https://www.washingtonpost.com/.

[22] Rid, *Active Measures*, 426.

[23] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2003); and Stephen Gerras et al., *Strategic Leadership Primer* (Carlisle Barracks, PA: US Army War College, 2010), 11.

Information Fires Team

The following paragraphs outline what combatant commanders require of personnel and a concept of operations to compete in the information domain. The skills described immediately below resemble that of good journalists and, in some cases, it may be possible for all these traits to exist in one person. More likely though, an organization engaged in information warfare will need a group comprised of individuals with these skills—an "information fires" team that acts as an anti-disinformation unit.

Such a team should be a part of the military and diplomatic instruments of power. But in the reality of ongoing military operations, military decision makers tend to feel most comfortable with and have confidence in the military members involved in a mission. This is especially true considering the Joint Force's advocacy of mission command principles that aim to "build teams through mutual trust."[24]

Military personnel would not necessarily perform the tasks outlined below better than a civilian diplomatic unit, but military personnel in combat operations are often thrust into positions where they must counter disinformation in the course of their military responsibilities. Additionally, the established martial mindset focused on targeting and kinetic fires aligns more closely with the military than with the diplomatic skillset. If senior military officers, therefore, find themselves in a position to rebut adversarial disinformation, having the right composition of individuals versed in current and historical geopolitics, metacognition, sense making, and communication should assist them in doing it more effectively.

Geopolitics

First, individuals in an information fires team should have a working understanding of regional history and the present geopolitical context, as the former so often informs the latter. Foreign area officers typically possess such skills and education. These individuals should also be able to think predictively. Too often, military members conducting combat operations focus on tactical events, or as some have termed it, "descriptive intelligence," which attempts to explain what just happened.[25] Fewer can describe why it happened. Fewer still offer a judgment regarding what will happen next. Those that do prognosticate do so without consequence—rarely can they point to empirical evidence of past predictive forecasting success.[26]

[24] Department of the Air Force, Air Force Doctrine Publication 1: *The Air Force* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, March 10, 2021), 2, https://www.doctrine.af.mil/.

[25] Ronald D. Garst, "Fundamentals of Intelligence Analysis," in *Intelligence Analysis*, ANA630, vol. 1 (Washington, DC: Joint Military Intelligence College, 2000), 18–28.

[26] James M. Davitch and Robert D. Folker Jr., "Operationalizing Air Force Critical Thinking," *Air & Space Power Journal* 31, no. 4 (Winter 2017).

Therefore, a robust knowledge of the geopolitical situation is critical for thinking about the future. Proving one's predictive bona fides through rigorous testing and evaluation is ideal. The Intelligence Advanced Research Projects Activity's "Good Judgment Project" showed how this type of program can produce impressive results.[27] A significant body of scholarship backs up the utility of using forecasting competitions, and more investment in this area across the Department is crucial.[28]

Metacognition

Second, individuals should be versed in metacognitive tools and theory. History has shown some of the most consequential military events hinged on how much our unconscious biases have influenced our decisions.[29] The military therefore requires those who understand not only what common cognitive biases to which they are personally most prone, but also the biases that may affect decision makers in their chain of command.

And because the enemy gets a vote, team members should also offer prescriptions informed by historical and geopolitical understanding to explain an adversary's potential thinking and possible reactions. This is especially critical with respect to coercion theory and deterrence operations. The dominant variable in structuring adversary incentives is the enemy's perception.[30] Too often, US deterrence operations forget this point despite Robert Jervis' warning that "what matters in sending a message is not how you would understand it, but how others will understand it."[31]

Open Source Information

Third, the individuals must be able to use information technology to sense-make by harnessing publicly available information. The expensive airborne or space-based sensors the United States used during the Cold War to gather information were and are important for certain needs. But today information flows freely through social media and other digital platforms.

[27] Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Random House, 2016).

[28] See Barbara Mellers et al., "Psychological Strategies for Winning a Geopolitical Forecasting Tournament," *Psychological Science* 25, no. 5 (2014); Philip Tetlock et al., "Forecasting Tournaments: Tools for Increasing Transparency and Improving the Quality of Debate," *Current Directions in Psychological Science* 23, no. 4 (2014); Tetlock, Mellers, and J. Peter Scoblic, "Bringing Probability Judgments into Policy Debates via Forecasting Tournaments" *Science* 355, no. 6324 (2017); and Welton Chang et al., "Developing Expert Political Judgment: The Impact of Training and Practice on Judgmental Accuracy in Geopolitical Forecasting Tournaments," *Judgment & Decision Making* 11, no. 5 (2016).

[29] Daniel Kahneman and Jonathan Renshon, "Why Hawks Win," *Foreign Policy* (2007).

[30] Tami Davis Biddle "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* 3, no. 2 (Spring 2020).

[31] Robert Jervis, *Perception and Misperception in International Politics*, new ed. (Princeton, NJ: Princeton University Press, 2017) 187.

Ralph Clem has plead repeatedly for the intelligence agencies to begin to give greater credence to information available in the public domain. He cites not only the ubiquity of valuable information but the technical sophistication of the exploitation tools available to citizens or public corporation.[32] In today's information environment, America risks losing the fleeting opportunities to seize the narrative if its military fails to use this readily available data source to characterize the environment.[33]

Communication

Fourth, the individual must be able to communicate clearly a picture that is truthful, accurate, and understandable to multiple audiences. Many military members are proficient at explaining a combat situation to other military personnel. Few have the skill to illustrate it in such a way that it, at once, provides deterrent value to an adversary and explanatory value for the public.

This skill set gets to the crux of the dilemma of military operations below the threshold of open conventional conflict. The right individuals possess the written and verbal faculties to reassure friends and family at home that America and her coalition allies' actions are justified while at the same time warn enemies their belligerence will not go unnoticed or unanswered.

Communication skills in the information environment will benefit from personnel that have a wide breadth of experiences, reflecting the reality of geopolitical challenges the military faces. For instance, the White House's *Interim National Security Strategy* clearly articulates how the characteristics of US Indo-Pacific Command's peer competitor challenges in East Asia vary considerably from the instability US European Command faces along Russia's near abroad. Versatility will be key and breadth will be more valuable than depth.

Yale historian John Lewis Gaddis, employing the Greek poet Archilochus's fox and hedgehog analogy, shows that individuals who possess a broad knowledge base (foxes) may be superior at operating across multiple problem sets. Gaddis argues nimble foxes are more comfortable in complex environments. (While Gaddis's assessment of the meaning of the analogy is not necessarily universally embraced, the proposal that breadth is more valuable than depth, especially in this context where communication is important, has merit.)[34]

This view of foxes contrasts with hedgehogs who possess only one area of narrow expertise. From the perspective of active duty members in defense intelligence, a broad rather than narrow knowledge base is much more beneficial, because it results in a more cogni-

[32] Ralph S. Clem, "MH17 Three Years Later: What Have We Learned?," War on the Rocks, July 18, 2017), https://warontherocks.com/.

[33] James M. Davitch, "Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data," *Joint Force Quarterly* 87 (2017).

[34] John Lewis Gaddis, *On Grand Strategy* (New York: Penguin Books, 2019); and James M. Davitch et al., "Lead, Think, and Communicate: Embracing Air Force Intelligence Officer Agility and Versatility," Over the Horizon, June 6, 2018, https://othjournal.com/.

tively versatile and agile military professional.[35] In the information fight, it is likely versatile foxes will be more useful when communicating information to multiple audiences.

Risk Management

Lastly, the individuals involved in this information fires team must accomplish these tasks balancing urgency, operational security, and accuracy. In this fight for public opinion, the strictures of operational security are and will be in tension with the need to rapidly control the narrative. While combatant commands may desire to move swiftly and gain the first-mover advantage, individuals indoctrinated in a culture of secrecy will be hesitant because their muscle memory will act contrary to the need for speed.

There is no simple answer to this problem other than both sides of the dilemma accepting risk. Commanders who want to "go fast" must reassure those under them that the risk falls on the commander when information is released. And those producing the information must find the most advantageous way possible to provide information, primarily from publicly available sources.

In his book *Active Measures*, Thomas Rid considers the history of Cold War information campaigns on both sides of the East/West divide and concludes it took a special kind of operator to excel in a disinformation environment.[36] That individual is something of a nonconformist, someone with a mind that works unconventionally. He or she enjoys exploring contradictions. They do not become frustrated by the lack of measurable success, as information warfare does not lend itself to typical metrics the military uses to assess effectiveness.

Finding individuals with these traits via current Department of Defense personnel systems would be difficult. Finding one person with all the traits would be harder still. Nevertheless, emerging software tools like the Air Force's "MyVector" are promising and provide more talent management utility than ever before. Military personnel agencies could assist the talent management search by studying, and possibly rewriting, the entries in their accessions guidance.

Current career field management teams should relook at their accessions guidance and determine if they may too strongly favor undergraduate science, technology, engineering, and math (STEM) degrees. The trade-off—that the career field might forfeit officers who are more technically minded—is acceptable because nontechnical degrees may be able to contribute more than commonly thought to building leaders with critical thinking skills.[37]

For example, the Air Force Officer Classification Directive uses a matrix to designate various tiers that outline which academic degrees the career fields value. Currently

[35] Davitch, "Agility and Versatility."

[36] Rid, *Active Measures*.

[37] Davitch and Folker, "Critical Thinking."

only 1 of 37 Air Force officer career fields listed denote those with cultural studies degrees as a tier-1 accessions target. Most of the desired degrees are STEM related.

As an aviation-centric military service, this is entirely appropriate. But one result from this relative deemphasis on cultural literacy is that for certain assignments, the Air Force must rely on individuals who attend midcareer foreign area training and may not have an academic grounding in social sciences. If the US military decides that cultural fluency is worth having as a small part of its information-operations approach, then slight modifications to its accessions targets could result in important changes to the types of personnel available for information fires teams.

A Concept of Operations

Once individuals with the correct skill sets have been identified and the in-garrison and deployed billets have been coded correctly, the information fires team needs a concept of operations. Fortunately, the kinetic targeting process that exists today provides just such a concept and only requires slight adjustments for information warfare. In short, we have done this before.

The goal of deliberate targeting is to ensure that the destruction of a target meets the commander's intent while adhering to the laws of war and rules of engagement. Targets nominated for kinetic and nonkinetic effects move through a validation process.

Deliberate targeting efforts follow a general pattern called the Joint targeting cycle, which is a framework consisting of six steps: (1) end state and commander's objectives; (2) target development and prioritization; (3) capabilities analysis; (4) commander's decision and force assignment; (5) mission planning and force execution; and (6) target assessment.[38] It is important to stress here that the Joint targeting cycle is a framework upon which information fires teams can build. Indeed, there are instances where the targeting cycle does not align with information warfare requirements.

First, due to the fluid nature of the information environment, a checklist-style method for employing information effects would be detrimental. Second, and this is true for many traditional targeting operations as well, targeting cycle steps can and often do happen concurrently. Ultimately, information fires teams should use it as a guide to synchronize their efforts in line with the commander's larger scheme of operations. Information fires must act in concert with, rather than independent of, combatant commander strategic guidance. Effective information fires modeled on the Joint targeting cycle will lead to the effective employment in the information warfare fight.

An information fires team will have the greatest ability to contribute within the competition-below-armed-conflict environment, whereby "two or more actors in the international system have incompatible interests but neither seeks to escalate to armed conflict."[39] It is here that the possibility for misperception and inadvertent escalation is

[38] Currently access is limited to *Joint Targeting*, JP 3-60, the document containing the Joint targeting cycle.

[39] CJCS, *Joint Operations*, JP 3-0 (Washington, DC: CJCS, October 22, 2018), https://www.jcs.mil.

the highest. Accordingly, using information fires in the grey zone will allow commanders to gain an advantage in the informational domain, put an adversary at an informational disadvantage, and help prevent conflict escalation while returning the geopolitical situation to a status quo condition.

Situating an Information Fires Team

An information fires team must be placed at the right level of warfare to contribute timely and effectively in support of a Joint Force commander. An argument can be made that it should reside at the strategic level because the team would receive combatant commander-level guidance in support of combatant command priorities. Yet if the team's purpose is to support the goals of the Joint Force commander, a combatant command-level organization could be in a position of serving two masters—the combatant commander and the Joint Force commander, if they are separate individuals.

At the other end of the spectrum, a tactical-level information fires team could adopt a small-unit-style operations tempo, like a fighter squadron, and respond at the pace of unit-level operations. But an information fires team at the tactical level could become too divorced from theater commanders' operational-level schemes of maneuver.

The most effective level of implementation, then, is operations, and the right unit for an information fires team is the Air & Space Operations Center (AOC). These centers already execute the Joint targeting process—the information fires team could operate easily within current targeting procedures. Additionally, Joint forces are already present in AOCs, notably US Army battlefield coordination detachments. Certain AOCs have already implemented "nonkinetic" targeting teams that could be modified for the purposes outlined in this article.[40] This model could be replicated at AOCs throughout the world.

Information fires teams should work within the AOC construct in support of theater component commanders. The US Air Force Air Combat Command should implement this concept, because information fires teams can assist in shaping the Air Force contributions in support of theater commander priorities. Such narrative building is, and will continue to be, vital to sustaining friendly coalitions. Additionally, these narratives will assist in weakening adversary narratives in competitions short of war.

Conclusion

The Air Force can lead the US defense enterprise as it uses truth to shed light on falsehood and proclaim the righteousness of the principles it fights for. Presenting the truth with forthright conviction and in a timely manner can help gain the first-mover advantage in the information space and deny it to adversaries. Doing so will allow those

[40] Jeffrey C. Crivellaro, *Combined Arms in the Electro-Magnetic Spectrum: Integrating Non-Kinetic Operations* (Fort Leavenworth, KS: Army School of Advanced Military Studies, May 23, 2013).

engaged in the profession of arms to maintain public support, foundational to preserving technological advantages. Military professionals will remain vital to the defense of the United States by gaining and maintaining the moral high ground. Force packaging teams of individuals with the cognitive skills identified above will allow the United States and its coalition partners to win in the information contests of the future and gain an edge over their adversaries.

Lieutenant Colonel James M. Davitch, USAF

Lieutenant Colonel Davitch holds a master of science in airpower strategy and technology integration from Air University and a master of arts in interdisciplinary studies from the University of Oklahoma.

Disclaimer and Copyright

The views and opinions in *Air & Space Operations Review* (*ASOR)* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *ASOR* editor for assistance: asor@au.af.edu.