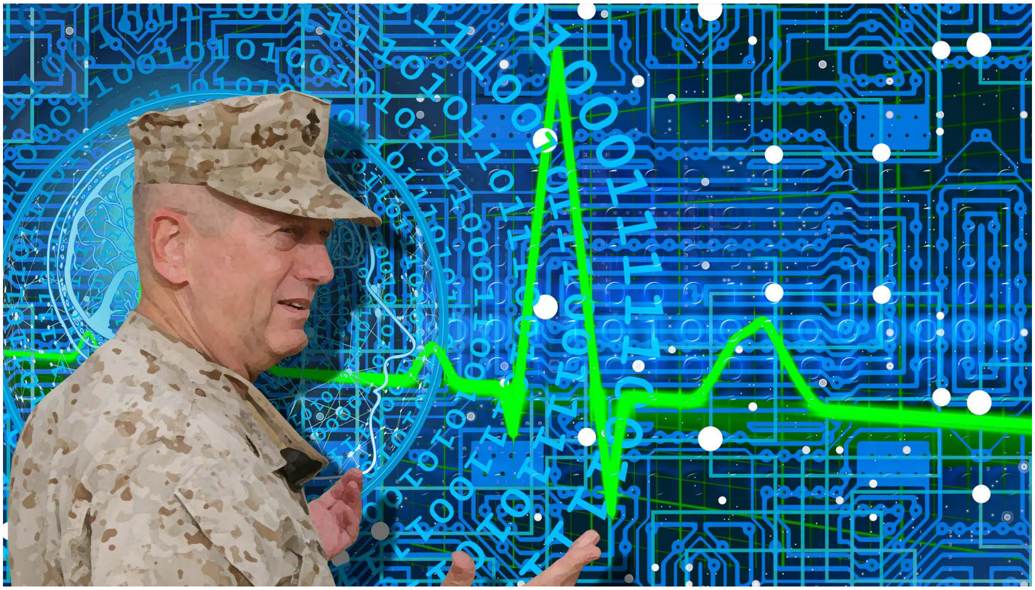
AIR & SPACE POWER JOURNAL - FEATURE

Information Warfare

Tuning Our Instruments to Overcome Barriers to Battlefield Harmony

Col Nathaniel Huston, USAF
Capt Keegan Newton, USAF
Capt John Runge, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.



Introduction

> *I don't care how operationally brilliant you are; if you can't create harmony—vicious harmony—on the battlefield, based on trust across different military services, foreign allied militaries, and diplomatic lines, you need to go home.*
>
> —Gen James Mattis

Battlefields are complex places, as Gen Mattis so eloquently pointed out in his recent memoir, *Call Sign Chaos*. Though the former defense secretary was reflecting specifically on the trust built between commanders in the run-up to *Operation Iraqi Freedom*, he rightly observed that the need for trust extends to all levels and forms of war fighting. Each pilot must trust his wingman, each soldier must trust his squad members, each commander must trust her fellow commander. Similarly, force employers and enablers must build trust between other employers and enablers. The bomber pilot must trust the targeteer to mensurate an aim point with precision, the fighter pilot must trust the tanker will fill her aircraft with nothing but the highest quality jet fuel, and the logistician must trust that the defender will keep his base safe. War fighting, quite simply, is an exercise in trust.

Today's war fighters face especially acute and compelling challenges regarding trust building. Similar to their forebears of 100 years ago—when the world's militaries grappled with how to effectively integrate war fighting from and through a new air domain—today's Airmen, Soldiers, Sailors, and Marines must compete on a battlefield altered by the introduction of an unfamiliar new domain, one that can be hard to conceive of, let alone integrate with. Recognizing this challenge, the US military has, during the past decade, significantly increased its institutional and operational capabilities in cyberspace and across the information warfare (IW) landscape.[1] One need look no further than the designation of US Cyber Command as our nation's 10th combatant command, for example, as a signal of the importance placed on the new domain.

Be that as it may, new organizations are not, by themselves, enough. To achieve the full potential of emerging technologies and fully exploit this new domain, warfighters on both sides of the digital divide must fundamentally adapt the ways in which they exploit their warfighting means. Simply employing new technology is not enough; the organization itself must change how it approaches the battlefield if it is to have success upon it. Today's warfighters face an inflection point, one in which trust plays a pivotal role. To borrow a phrase from our special operations brothers and sisters, for the US to be successful at operating *by, with,* and *through* the information environment, we must intensify integration efforts and eliminate barriers that prevent building the trust necessary for the vicious harmony we seek to achieve.

This article argues there are three primary barriers that prevent the effective integration, synchronization, and convergence of IW capabilities with each other and, perhaps more importantly, with the broader spectrum of multidomain capabilities. First, IW integration is hampered by the lack of a common lexicon, both within and between IW functions and between IW and other war-fighting elements. This not only prevents efficient internal and external synchronization but also obscures how IW complements full-spectrum operations. Second, IW suffers from a tendency to over-classify information that prevents operational decision-makers from understanding, integrating, and leveraging IW capabilities. Finally, although progress has been made, authorities to employ IW capabilities are still widely held at high levels that inhibit war fighting agility and diminish the potential impact of these capabilities. Many seek the path to the successful integration of our disparate IW functions and further, to their integration and synchronization with the broader spectrum of military capabilities; breaking down these barriers promises to accelerate this vision's timeline.

Indeed, following that path and achieving vicious harmony is critical on today's battlefield, one that remains increasingly interconnected through the advancement and employment of information technology. In today's information age—where war fighters are surrounded by screens, sensors, control devices, and signals—trust and harmony are crucial to success. Whether in the avionics back shop of an F-15 hanger, accessing Predator feeds from a handheld Rover device, or monitoring network operations on a standard Windows workstation, cell phones, smart watches, and computers abound. These devices are sending and receiving signals almost without stop. Although technology has provided increased work capacity and convenience, it also introduced a new contested domain that can be exploited for warfighting purposes. Our adversaries have already begun to capitalize on the potential for military operations through the information environment and are actively developing strategies to take advantage of it.[2] To maintain (or as some have argued, regain) a position of relative advantage, the United States must make every effort to maximize the unified potential of cyberspace operations (CO), information operations (IO), electronic warfare (EW), and intelligence, surveillance, and reconnaissance (ISR).[3]

With respect to our argument, it is with these information-related capabilities (IRC) that we wish to spend the most time in contemplation below. Relative to IRCs, "traditional" military capabilities—those that exist mostly in the physical dimension—tend to be easier to trust, most simply because they are easily perceived by our senses.[4] One can hear and feel the roar of an F-22 as it conducts a defensive counterair sortie. One can see the "boots on the ground" of the soldier occupying enemy territory. IRCs on the other hand, have yet to earn the same level of operational trust.

IRCs can be difficult to understand, and their accesses and effects are often plagued by increased uncertainty relative to their often more explosive counterparts. They are rarely visible to the human eye, requiring instead the interpretive lens of a workstation. Their ethereal nature often means that earning trust is an inherently uphill battle. It is all the more imperative, then, that to the extent possible, barriers preventing harmony be removed. The first barrier, which prevents effective communication, is perhaps the most basic but also most challenging to overcome. Absent a common lexicon, IW operators often struggle to communicate with each other, let alone with those outside the virtual world in which they travel. This situation hampers their own understanding of how they fit within the overall mission and often hinders "outsiders" from accurately perceiving the reality of what the IW community has to offer.

Barrier One: Communication

Many readers are likely familiar with the old trope that goes something like, "communicators are the worst at communicating." Long have the so-called computer nerds of the military suffered the ill effects of "tech-itis," chief among them the peculiar malady of a vocabulary increasingly consisting of beeps and squeaks. This situation can be expected, to some extent, as any profession naturally develops a distinct vocabulary, a shared language of implicit meaning, and shortcuts allowing efficiency of communication. IW career fields are no different; as they evolve, they naturally develop a language that allows them to more effectively communicate within the ones and zeros of the information environment. Just as pilots have developed an understanding of their domain and concomitant vernacular, cyber operators—as they have professionalized and come to understand the information environment—have developed their own language of operations. While this is to be expected, and indeed even celebrated as the career field matures, it offers challenges that, if not addressed, promise to hinder trust, integration, and, ultimately, battlefield harmony. The lack of a common lexicon impedes integration among IW providers, frustrates their ability to understand how they fit within the multidomain fight, and finally, can lead to their exclusion from without, as others struggle to perceive their value to the joint fight.

First and most fundamentally, a new lexicon is only useful to the extent that it is a *common* lexicon. Although many of the beeps and squeaks of the cyber environment are similar, their operationalization can tend to constrain practitioners in silos of self-identification that separate them from the war fighting identity they share with their fellow men and women in uniform. This is of course true in any military domain; as Sun Tzu reminds us, knowing one's enemy is critical to success on the battlefield. Sun Tzu also counsels, however, that one must also know oneself, and in an environment in which war fighting looks so different, the importance of common language is heightened. CO tends to live within organizational constructs and use naming conventions that reflect their unique relationship within the information environment. Roles include technical directors and exploitation leads, each of which have specific roles and responsibilities to the mission.[5] EW, on the other hand, organizes its operations in the electromagnetic spectrum around the concepts of electromagnetic attack, electromagnetic warfare support, and electromagnetic protection.[6] IO offers yet another conceptual framework from which to perceive operations in the information environment, referencing "actions taken to affect adversary information and information systems while defending one's own information and information systems."[7] Understanding how these concepts relate to and differ from one another is critical to integrating their effects against an adversary and is not easily accomplished between the IW functions themselves, let alone between IW functions and the larger joint force.

To be sure, there is a place for specialized and precise lexicon. Within the context of IW, however, the independent growth of this myriad of functions has led to a panoply of vocabularies that make communicating between them difficult, leading to a second and equally concerning challenge. Without a common lexicon, it can be hard for IW practitioners to understand their place within their own service or the larger joint mission. A common lexicon can help to define not just one's own processes and identity but how that identity fits within its larger organization.

The Marine Corps Planning Process, for instance, helps unify Marines around a common concept of maneuver warfare.[8] Whether driving a tank, flying a helicopter, or storming a beach, a Marine's place within the Marine Air-Ground Task Force (MAGTF) is defined by his relationship to his fellow Marines and as such, to the larger joint force. Marines are taught from an early point in their careers how the functions of the MAGTF work together in a synchronized and integrated way. Similarly, military aviators share a common language and lexicon while still specializing in—and speaking about—their own specific weapon systems in unique terms. Simply put, these communities have professionalized their approach to war fighting individually but also collectively. We cannot yet say the same of those operating within the IW environment.

As IW advances and the entire community professionalizes, practitioners across the various functions must undertake to find common ground and institutionalize their approach, just as any professional community would. To the extent possible, the community should seek to integrate its own language and practices into those of their joint partners. "Dropping cyber bombs" may be an unhelpful and perhaps unfortunate euphemism, but one need not throw the baby out with the bathwater when it comes to integrating and normalizing language.[9] Concepts like joint fires, movement and maneuver, and protection certainly might not map as precisely onto the information environment as they do to physical realm, but they are doctrinal and, most importantly, shared. These terms allow war fighters to communicate between and across functions, which provides tighter integration and synchronization. A concerted effort to create a common vocabulary and fit it within these shared concepts is a good way to professionalize within IW and maximize its potential within the joint force.

To some extent, the stand-up of Sixteenth Air Force (Sixteenth AF) has begun to alleviate this challenge—for the Air Force at least—by offering those within it a single organization from which to derive their identity and, as such, comprehend their position within the larger war-fighting construct. In a recent interview General Haugh, the first and current commander of the newly activated Sixteenth AF, referenced the need to integrate these disparate functions as the impetus of the organization's creation.[10] As the organization matures, it will be important for its members to conceptualize not just how they relate to others within the IW community but also how they all fit into the larger organization of the US Air Force and indeed, the entire joint force. This is all the more imperative for those operating within the information environment, where self-imposed boundaries between services quickly fade away from an adversary's perspective. A common lexicon among and between IW professionals will help sharpen their perception of where they fit and facilitate synchronization of effects across the spectrum of operations, allowing the whole to become greater than the sum of its parts and invigorating the trust upon which victory on the battlefield must rest.

In addition to a sharper self-perception, this foundation is crucial to build "outside-in" trust; that is, trust *from* outside of the IW community *in* what the IW community has to offer. Sixteenth AF offers those within it a shared identity but from the outside, Sixteenth AF is a lot of things to a lot of people. In the same interview, General Haugh referenced no fewer than 10 significant and wide-ranging missions for which he is responsible.[11] In many ways, what IW means to an individual is derived from where that individual sits organizationally and what slice of IW is most significant to that organization, which leads to the final challenge facing an IW community without a common lexicon: without the ability to speak the same language, IW operators struggle to speak with a single voice and, as such, struggle to communicate their value to the larger joint force. This is not to say that they are *un*valued, but simply that when IW is so many things to so many people, it can be hard to accurately perceive its full potential when properly integrated.

Here again, the stand-up of a consolidated organization in the Air Force offers a promising first step to helping "outside" customers recognize how IW functions fit within the larger range of military operations. ISR capabilities, for instance, have progressively become more assimilated across all mission types. Full-motion video has become an almost-expected commodity among war fighters across the services, and battle damage assessments, always critical to determining the effectiveness of a given operation, have become tightly integrated throughout the joint force. As those functions have matured, their lexicon has matured to communicate effectively and efficiently with joint partners to enable a level of synchronization not as widely enjoyed across the rest of the IW spectrum. Learning from this example and building on this strength will help elucidate the value the entire IW community brings to the joint fight.

Barrier Two: Classification

Sun Tzu counsels, "Conceal your dispositions, and your condition will remain secret, which leads to victory; show your dispositions, and your condition will become patent, which leads to defeat."[12]

Today's information environment is nothing if not Sun Tzuian, at least in this respect, perhaps to a fault. Although well-intentioned, many operating within the domain suffer from a predisposition to protect rather than share, which has resulted in an environment of over-classification that threatens to undermine the effectiveness of the very systems we seek to protect.[13] This is understandable, of course. From very early in their careers, war fighters privy to classified information are correctly trained that security of resources, access, sources, and information is paramount to operational security. Vigilance, in protection and secrecy, is critical to the preservation of the nation's technological edge and position of strategic advantage, such that those exist. Those with security clearances are keenly, and appropriately, aware of the repercussions of under-classifying material—both from an operational standpoint and a personal standpoint. Risk must not be taken unnecessarily.

War fighting, however, involves risk, at least to some extent. There is a cost to "playing it safe" and erring on the side of caution. Over-classification of material not only erodes public trust in military processes and costs an estimated amount of billions of dollars every year, but hinders effective war fighting.[14] This is especially true in the information environment. If mission partners within and external to the IW community cannot access critical information due to over-classification, IRCs cannot be effectively and harmoniously integrated into the twenty-first century battlespace. IW becomes a victim of its own sensitivity.

This is not, of course, a problem unique to the IW community. General John Hyten, the vice chairman of the Joint Chiefs of Staff, told the audience at an Air Force Association event that "in many cases in the department, we're just so over-classified it's ridiculous, just unbelievably ridiculous." General Hyten related a story in which, when he was head of US Strategic Command, he invited the then-head of US Pacific Command, Adm Harry Harris, to a briefing that was so classified, even their deputy commanders, both three-star flag officers, were not allowed in the room.[15] General Hyten lamented that if "the only people in the room are four-stars, you really can't get any work done."[16] His point, and the point of our own argument, is that classification of information always involves weighing risks and rewards; it involves tension between safeguarding information from the enemy and ensuring the right information gets to the right people to prosecute the enemy. The challenge is ubiquitous in the IW environment.

Similar to the first barrier, the over-classification barrier is inherently a communication challenge that has the potential to impact successful mission execution. How can planners practically integrate IRCs without fully understanding those capabilities or, at a minimum, the basics of how they work, their effects, and their dependencies? The bulk of today's operational planning and execution occurs at the Secret level. Most of the capabilities that planners consider for air and ground operations can be found on unclassified or Secret-level networks. This gives all planners the opportunity to understand these capabilities and build a plan around them. This is not the case with IW capabilities, which are usually not only highly classified, but also often require special accesses. The negative effects of over-classification manifest at the tactical, operational, and strategic levels, but at the lowest levels, integration is significantly hindered by the inability to share during operational planning.

In addition to its negative impact on planning, over-classification negatively impacts the potential of the IW community to earn operational trust. If fellow war fighters are not given enough information to understand various IRCs, trust is very difficult to gain and, along with it, the effective utilization of those capabilities on the battlefield. In the absence of confidence in IW capabilities, war fighters understandably default to traditional military capabilities, those they can feel and hear and whose effects are directly observable once the smoke clears. Without trust, IW operators risk handicapping their own effectiveness. In a business in which effectiveness is often measured in lives lost, these costs are simply too great to bear unnecessarily.

The good news is, in this challenge IW professionals are not alone. The space community, for instance, has long faced a similar challenge of trying to integrate highly classified capabilities. Information about these capabilities must be protected to prevent undermining their operational effectiveness, but leaders within what is now the US Space Force have recognized the need to empower their operators in order to improve war-fighting efficiency, which required communication lines to be less restricted. To achieve this, leadership probed the issue from several angles. What information can be made unclassified? What information can be made nonprogram classified? And, instead of single-access programs, could umbrella-access programs be created? With these questions in mind, and the understanding that an inability to adapt would cause continued inefficiencies and the potential for adversarial surprise, the space community has made progress on loosening classification restrictions.[17] Unsurprisingly, this change has been a catalyst to better enable the joint force to integrate its arsenal of capabilities.[18]

The IW community faces similar challenges. How can IW practitioners effectively communicate and work with the joint force if they are not able to access IW resources at the places where the fight occurs? The issue is being addressed, and the Chairman of the Joint Chiefs of Staff has directed a re-evaluation of our classification guidance.[19] In the meantime, IW planners might help by creating an IW playbook (a database of sorts) containing summaries of existing capabilities that is accessible at the Secret level and across the operational community. This repository could also list "best practice" integration techniques across the spectrum of IW capabilities. It could, for example, explain how ISR could be leveraged to work in concert with CO to deny an adversary's access to a given communication link or platform while at the same time using IO to create a leaflet campaign telling civilians to not use that link or platform. If such a repository currently exists, institutionalization of its use across the joint planning enterprise could increase its usefulness.

Gen Mattis once suggested that he had "never been on a crowded battlefield, and there is always room for those who want to be there alongside."[20] Ultimately, sensitive information must be protected, but in a manner that allows cooperation among and between mission partners. If classification decisions come at the expense of military progress and dominance in IW, they must be made deliberately and with the knowledge that they come at a real cost. Military members, even those operating in the virtual battlespace, are in the business of fighting wars, and war fighting involves risk.

Make no mistake, the argument is not to lower classification levels across the board. Rather, the intent is to arm commanders and planners with an increased knowledge of how IW capabilities can be integrated into the fight. Ultimately, the desire is to pave the way for expanded knowledge at lower levels for increased authorities to be delegated. Expanded knowledge of capabilities paves the way for increasingly informed and deliberate decisions regarding risk that are able to be made at progressively lower levels—levels that cannot today be trusted to make informed decisions often because they have no knowledge of the capability itself, let alone risk associated with employing it. As we give a little in making the knowledge of these capabilities available at a lower classification level, we gain a little in the way of trust by the joint force.

Barrier Three: Authorities

The final barrier at issue is one near and dear to many cyber operators' hearts. Seemingly since the first bit was fired in anger, many have lamented what they perceive to be an overly-restrictive approach to employing cyber capabilities, one that holds authorities at a level so high as to prevent many operations from being executed in a timeframe short enough to be effective.[21] Those familiar with the debate, of course, will know that there are very good reasons for the seemingly overly-restrictive approach. Often, decision-makers must decide whether the benefit from an operational effect outweighs the potential benefit of continued access to a given source of intelligence.

Additionally, there are very real legal issues that remain unresolved regarding where to draw the line between Title 10 and Title 50 actions when it comes to operations in cyberspace.[22] Further, IRCs are often costly to develop in terms of access, time, and money. Regardless of any debate about continued intelligence exploitation, simply using a given capability can highlight a vulnerability, thus nullifying the IRC's potential for future effects and therefore increasing the "per unit" cost of the weapon exponentially. Finally, given the nature of the information environment, operations in cyberspace offer exponentially higher risk posed by what has come to be known as the "strategic corporal," a war fighter who, though operating at a tactical level, may have strategic and political effects. While many in the US military have recognized and actually begun trying to leverage this new reality, the nature of operations in cyberspace remain at risk of resulting in outsized and unintended effects and as such, trepidation remains with regard to pushing decision-making lower in the chain of command.[23]

Suffice to say, there are many good and just reasons to keep a wary eye on efforts to increase authorities at lower levels. Today's cyber warfare landscape, however, suggests that there are good reasons to take increased risk in this arena. The doctrinal emphasis China places on seizing the initiative as the "single most decisive factor in controlling and winning a war," or the extent to which Russia values swift actions during the Initial Period of War echoes the need to make decisions at an increased pace.[24] These sorts of challenges are not unique to IW, and we would be well-served to look to other force employment platforms to learn how to loosen restrictions and increase agility at lower levels while continuing to maintain a healthy respect for the risks incurred by doing so.

In the case of air warfare, for instance, a combatant commander carries the ultimate responsibility of calling strikes in his or her theater, but operationally pushes strike decision authorities lower down, to the battle director, at an air operations center. The intent is to shorten the kill chain, the process of rapidly understanding threats, making decisions, and taking military actions.[25] At times, even this chain of approval has proven too cumbersome for effective, "harmonious" combat operations. Facing real challenges with coordinating time-sensitive strikes on emerging targets, innovative air strategists in the 1980s developed what would become known as "kill boxes," essentially pre-coordinated three-dimensional areas wherein authorities to strike targets were pushed to a lower, more tactical level. Importantly, they were not conceived of as "free fire" zones, but were instead intended to be areas in which the rules of engagement were deliberately and purposely tailored to allow decision-making to proceed at a more rapid pace.[26] Today, the concept is enshrined in doctrine and is a standard part of the toolkit available to commanders and planners seeking to increase dexterity and empower war fighters to make time-critical, risk-informed decisions in the heat of battle.

Whither IW's "kill boxes?" What innovative solutions might the joint force be able to offer to mitigate the risk of unintended consequences while acknowledging the real need to increase agility on the part of cyber operators making split-second decisions and executing operations that at times quite literally occur at the speed of light? The importance of empowering war fighters at the operational and tactical levels is hard to overestimate. Gen David Goldfein, former USAF chief of staff, in fact, made revitalizing the squadron a centerpiece of his strategic vision.[27] In eliminating costly red tape in its processes and removing hundreds of outdated or frivolous instructions, Air Force leadership has liberated its war fighting force and pushed authorities down to lower levels, thus creating an environment more suitable to a shortened kill chain.[28] National Security Presidential Memorandum 13, signed in August of 2018, appears to be a good first step to loosening the reins in cyberspace.[29] It pushes authorities to lower levels and allows for a significant increase in the number of operations, but more work remains to be done to allow dexterity and synchronization while providing assurances that oversight will remain effective.[30] One process-related solution is the concept of a selection of Pre-Approved Actions (PAA) that enable commanders to take rapid, decisive actions on the battlefield in response to specific operational events or "triggers." This solution has begun to find its way into other areas of IW such as CO, but the capability is nascent and its future uncertain.[31] In any case, whether through virtual "kill boxes" or an invigorated approach to PAAs, IW requires innovation to allow the sort of increased, deliberate risk-taking that will increase agility and synchronization throughout the information environment.

Conclusion

We cannot know the way if we do not see the path. These barriers represent restrictions that create friction as we strive toward synchronization, integration, and ultimately, vicious harmony between the rapidly growing IW battlefield and the broader environment of military operations. For IW operators to breach these barriers, the Department of Defense (DOD) must take a serious look at the culture that has grown around the information environment of warfare. IW should focus specifically on identifying the ways in which commanders can be effective at delivering IW capabilities. In the DOD, we have initiatives to increase our ability to conduct IW by combining the effects of EW, IO, CO, and ISR in new and exciting ways. While the future state of synchronized, converged, and integrated IW capabilities is invigorating, we must first deal with our self-imposed, internal barriers to a successful campaign in the information environment.

There are three primary obstacles preventing achievement of the desired IW future state. First, IW practitioners have experienced difficulties in understanding the battlespace and lexicon within our own communities and those of the joint force, which has resulted in communication challenges, both internal and external to the IW community. Second, IW capabilities are frequently highly classified, which makes mission planning difficult, especially across a multidomain operation. If members across the planning process are not knowledgeable of a particular program or capability, decision-makers are understandably handicapped, and operations are potentially less effective. Third, although we are making progress pushing authorities to lower levels, more must be done to offer commanders creative ways to allow lower-level decision-makers the authority they need to become more agile. These barriers stand in the way of creating the vicious harmony necessary to maximize the potential offered via operations *by, with*, and *through* this new domain.

To overcome these barriers, we must aggressively push forward on several fronts. First, IW professionals ought to work hard to establish a common lexicon that will both increase their own understanding of how they fit into the larger war fighting effort and allow those outside the community to understand the value their capabilities offer. Further, leadership must continue to critically examine the risk versus reward of current classification requirements and their impact on our national defense. Simply put, IW dominance requires a more widespread understanding across the spectrum of planning and decision-making. This understanding can only be accomplished through making deliberate and informed decisions about where classification requirements can be relaxed. Finally, to match the speed at which war fighting can occur in cyberspace, operational and force employment decisions must, to the greatest extent possible, be pushed lower in the chain of command.

Importantly, much of what is advocated for above involves building a culture inside of IW that is comfortable with increased risk. Equally as important, the risk must not be unmitigated but rather deliberate and thoughtful. To the extent that victory upon today's battlefields hinges on America's ability to leverage IW capabilities more effectively than her adversary, we argue that the increase is justified. In order to capture significant technical gains, an organization must reward successful risk-taking and minimize penalties for failure. Unwillingness to take risk should be eschewed altogether.[32] In shaping our future, we should look to the examples of our fellow war fighters, those who have fought successfully for decades on land, air, and sea. We must professionalize, take risk, and build trust in order to achieve vicious harmony on tomorrow's battlefields. ✪

Col Nathaniel Huston, USAF

Colonel Huston (BS, MA, PhD, University of Notre Dame; MS, Air Command and Staff College; MPhil, School of Advanced Air & Space Studies) is a School of Advanced Air and Space Studies professor of strategy and security studies.

Capt Keegan Newton, USAF

Captain Newton (BA, BA, Virginia Polytechnic Institute and State University; MS, Iowa State University) is an operator on a Department of Defense Red Team.

Capt John Runge, USAF

Captain Runge (BA, University of Nevada, Las Vegas) is a 7th Intelligence Squadron assistant director of operations.

Notes

1. Sixteenth Air Force, "16th Air Forces (Air Forces Cyber)," 31 July 2020, https://www.16af.af.mil/.

2. Joint Publication (JP) 3-13, *Information Operations*, 20 November 2014, ix–x, https://www.jcs.mil/; and James Mulvenon and Richard Yang, *The People's Liberation Army in the Information Age*, RAND Report CF-145-CAPP/AF (Santa Monica, CA: RAND, September 1999), 175–86.

3. Dustin Weaver, "Lawmakers Fear US Has Fallen behind in Cyber Warfare," *The Hill*, 5 March 2017, https://thehill.com/; Peter Apps, "Commentary: As Cyber Warfare Turns 10, the West Risks Falling Behind," *Reuters*, 4 May 2017, https://www.reuters.com/; Gopal Ratnam and John Donnelly, "America Is Woefully Unprepared for Cyber-Warfare," *Roll Call*, 11 July 2019, https://www.rollcall.com/; Lawrence Sellin, "*The US Is Unprepared for Space Cyberwarfare,*" *Military Times*, 4 September 2019, https://www.militarytimes.com/; JP 3-12, *Cyberspace Operations*, 8 June 2018, vii, https://www.jcs.mil/; JP 3-13, *Information Operations*, 20 November 2014, ix–x; JP 3-13.1, *Electronic Warfare*, 8 February 2012, v-vi, https://fas.org/; and JP 2-0, *Joint Intelligence*, 22 October 2013, I-11, https://www.jcs.mil/.

4. JP 3-13, *Information Operations*, ix–x.

5. Maryse Penny, Tess Hellgren, and Matt Bassford, *Future Technology Landscapes: Insights, Analysis, and Implications for Defence* (Washington, DC: RAND, 5 December 2013), 77–79.

6. Curtis E. LeMay Center for Doctrine Development and Education, "ANNEX 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operations," 30 July 2019, 20–26, https://www.doctrine.af.mil/.

7. Herb Lin, "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations," *Lawfare*, 27 March 2020, https://www.lawfareblog.com/.

8. Marine Corps Doctrinal Publications 1, *Warfighting*, 4 April 2018, 3–9, https://www.marines.mil/.

9. Brandon Valeriano, Heather Roff, and Sean Lawson, "Dropping the Cyber Bomb? Spectacular Claims and Unremarkable Effects," *Council on Foreign Relations*, 24 May 2016, ***https://www.cfr.org/***.

10. Mitchell Institute, “Aerospace Nation: Lt Gen Timothy Haugh, Commander, Sixteenth Air Force, AF Cyber, & Joint Force HQ-Cyber,” 15 July 2020, *YouTube* video, 1:16:13, https://www.youtube.com/.

11. Mitchell Institute, “Aerospace Nation: Lt Gen Timothy Haugh, Commander.”

12. Sun Tzu, *The Art of War*, https://suntzusaid.com/.

13. Patrick Eddington and Christopher Preble, “Bad Idea: Overclassification,” *Center for Strategic and International Studies*, 6 December 2019, https://defense360.csis.org/; and Cathy Maus, “Office of Nuclear and National Security Information: History of Classification and Declassification,” *Federation of American Scientists*, 22 July 1996, https://fas.org/.

14. Eddington and Preble, “Bad Idea: Overclassification”; and Maus, “Office of Nuclear and National Security Information.”

15. Aaron Mehta, “Unbelievably Ridiculous: 4-Star General Seeks to Clean Up Pentagon’s Classification Process,” *Defense News*, 29 January 2020, https://www.defensenews.com/.

16. Mehta, “Unbelievably Ridiculous.”

17. Nathan Strout, “Barretts, Rogers Consider Declassifying Secretive Space Programs,” *Defense News*, 7 December 2019, https://www.defensenews.com/.

18. Nathan Strout, “Nominee to Lead Space Command Voices Support for Declassifying Space,” *C4ISRNET*, 28 July 2020, https://www.c4isrnet.com/.

19. Mehta, “Unbelievably Ridiculous.”

20. James Mattis, “Duty, Democracy and the Threat of Tribalism,” *Wall Street Journal*, 28 August 2019, https://www.wsj.com/.

21. Mark Pomerleau, “New Authorities Mean Lots of New Missions at Cyber Command,” 8 May 2019, https://www.fifthdomain.com/.

22. Robert Chesney, “Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries,” *Lawfare*, 12 April 2018, https://www.lawfareblog.com/.

23. Mark Pomerleau, “New Authorities Mean Lots of New Missions at Cyber Command,” 8 May 2019, https://www.fifthdomain.com/.

24. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).

25. Eric Jacobson, “Sino-Russian Convergence in the Military Domain,” *Center for Strategic & International Studies*, 22 March 2018, https://www.csis.org/.

26. JP 3-9, *Joint Fire Support*, 10 April 2019, A-9, https://www.jcs.mil/.

27. Gen David Goldfein, USAF, “CSAF Letter to Airmen,” 9 August 2016, USAF, https://www.af.mil/.

28. Stephen Losey, “Air Force Cuts 226 AFIs in Latest Salvo Against Hated ‘Queep,’” *Air Force Times*, 29 August 2018, https://www.airforcetimes.com/.

29. Mark Pomerleau, “New Authorities Mean Lots of New Missions at Cyber Command,” *Fifth Domain*, 8 May 2019, https://www.fifthdomain.com/.

30. Mark Pomerleau, “DoD Cyber Ops Are Changing, and so is Oversight,” *Fifth Domain*, 3 June 2019, https://www.fifthdomain.com/.

31. JP 3-12, *Cyberspace Operations*, IV-15.

32. The Space Archive, “RAW Elon Musk Interview from Air Warfare Symposium 2020,” 2 March 2020, *YouTube* video, 55:23, https://www.youtube.com/.