Soldier with Cyber Electromagnetic Activities section, 1st Armored Brigade Combat Team, 1st Infantry Division, points toward nearby objective during final day of training with section's new electronic warfare equipment, Fort Riley, Kansas, April 6, 2018 (U.S. Army/Michael C. Roach)

It's Not Just About Cyber Anymore

Multidisciplinary Cyber Education and Training Under the New Information Warfare Paradigm

By Joshua A. Sipper

Dr. Joshua A. Sipper is a Professor of Cyber Warfare Studies in the Air Force Cyber College at Air University.

Education and training have been complementary philosophical cognitive frameworks necessarily focused on harmonious, yet separate, areas of information delivery to people in a vast array of careers. Much research has compared and contrasted these two philosophies, revealing the need for an understanding of how best to target learning in order to accommodate the needs of students, of organizations in need of talent, and of society as a whole. The fact is that we need welders and plumbers just as

badly as we need doctors and lawyers. However, the way we train and educate across these vastly different career trajectories must by necessity flow and work in different ways.

The same could be said concerning education and training in the cyber career field. While cyber at a coding, hacking, systems administration, and applications level requires targeted training, education—which includes a more strategic and policy leadership bent—must be approached from a high-level, critical thinking vantage. There exist obvious similarities between training and education, such as a multidomain approach using cognitive, psychomotor, and affective strategies to promote learning. But the root philosophies have been and remain decidedly different. As Reginald Melton wrote, "It is important that we should not lose sight of the differences between education and training, for it is these differences that help us to keep the links clearly in perspective."[1] Yet there are also important links that must be maintained between education and training in order to communicate needs, standards, and knowledge, skills, and abilities (KSAs).

Cyber education and training are currently experiencing an unavoidable renaissance due to the inclusion of additional disciplines within the greater information warfare (IW) framework. This IW paradigm shift has been effected primarily by a natural confluence of information-related capabilities (IRCs), namely cyber operations (CO); intelligence, surveillance, and reconnaissance (ISR); electromagnetic warfare (EW); and information operations (IO). Each of these IRCs plays a distinct yet integral part in the IW superstructure, enabling military offensive, defensive, and exploitative operations at multiple levels. With this influx and cross-pollination of IRCs, education and training will necessarily take on new challenges as well as a transformation that will ostensibly enable joint all-domain operations (JADO).

Cyber Training and Education

As with any complex technical discipline, cyber training and education are connected and related at many levels. While these connections might serve to obscure where the dividing lines between training and education lie, they also enable the all-important multidisciplinary nature of cyber and the continued flow of cyber into and between ISR, EW, and IO within the nascent IW construct. Within the various military Services, however, technical cyber training and academic cyber education still maintain a necessary and complementary separation important for ensuring operational and organizational efficiency. As stated by Professor Melton, "Developing individual competencies to meet [industry] needs is what training is all about. . . . Meeting the totality of an individual's needs is what education is all about."[2] Both training and education are critical from this standpoint, as industry and individual needs must be met in order to ensure all gaps are closed. This is nowhere truer than in the cyber sphere, where organizations and individuals across the national, military, and state levels require technical and policy expertise on a near-constant basis.

With the demands currently placed on cyber in practically every corner of education, government, military, and corporate environs, ensuring the steady flow of network operability and a well-trained and well-educated workforce is not only challenging but also absolutely critical to maintaining security and operations. In order to effect this massive undertaking, cyber training and education must be understood individually, taking into account each area's subtle differences and strengths. Additionally, training and education overlap, and similarities within cyber specifically must be examined in order to find the common ground and interoperability necessary to continue the dominant nature of the U.S. military cyber panoply.

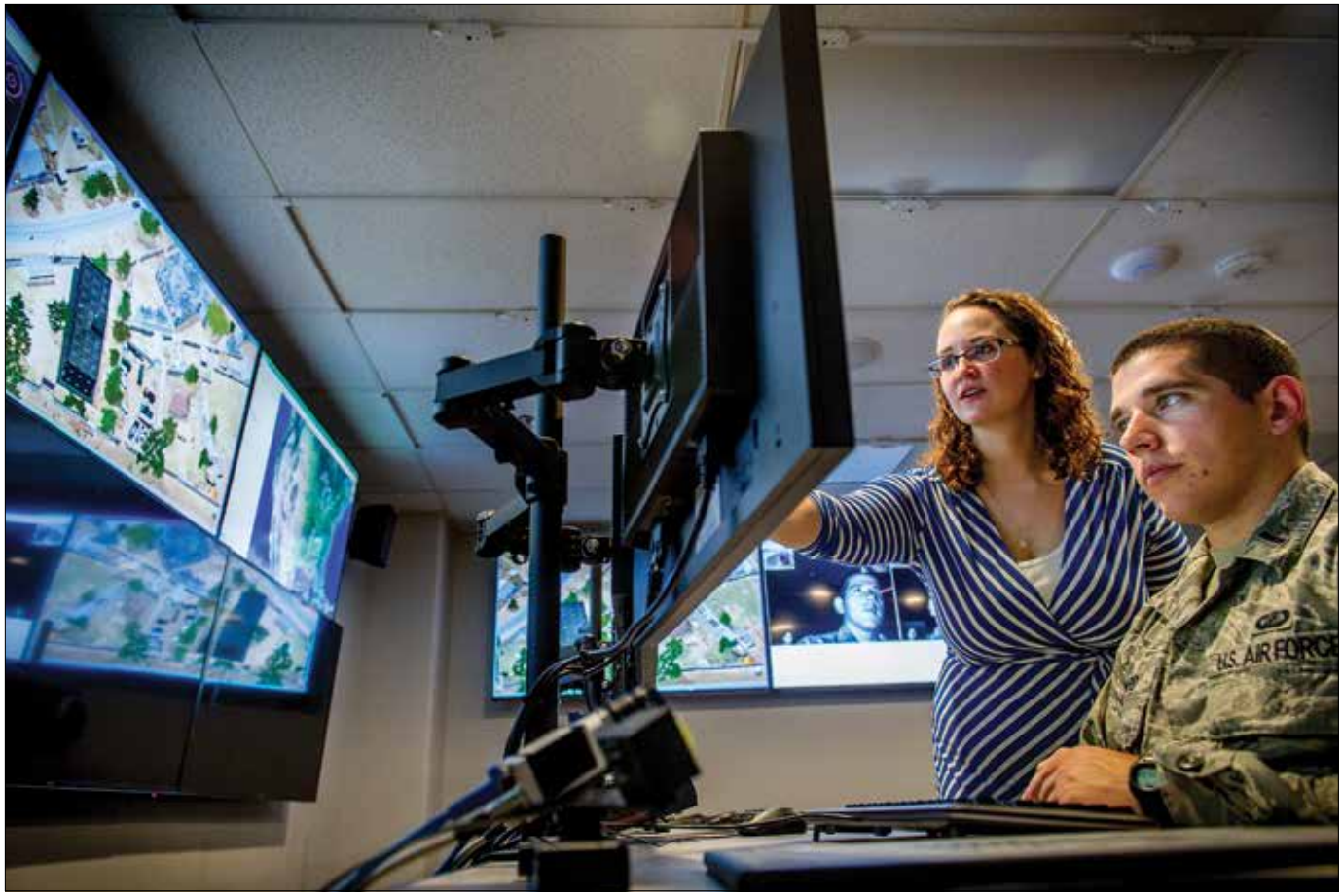
Cyber Training. Training is, at its core, about giving students the tools to accomplish tasks. With this understanding in mind, it is easy to see that the basic function of training is the development of competencies. Major General Burke Wilson and others discuss the need for Air Force cyber training in these terms: "A critical step towards normalizing cyberspace operations is the continued incorporation of advanced concepts in technical training school, which better equips our Airmen for the challenges they face in an increasingly contested operating environment."[3] Another issue foundational to keeping pace with the complexities and growth of cyberspace is a ready and expanding cyber professional force.

According to Francesca Spidalieri and Jennifer McArdle:

> *Compounding the shortage of highly trained cyber forces are the increasing scale, complexity, and continuous growth of DOD* [Department of Defense] *networks that are providing new avenues for adversary exploitation. In 2011, DOD cyberspace architecture was already the largest in the world, including over 15,000 networks and seven million computing devices spread across hundreds of installations globally. Today, the networks continue to expand, adding new features and assimilating new technologies, such as mobile devices and cloud computing.*[4]

The addition and proliferation of new technologies require expanded training and continuous learning across the joint force and within government and commercial sectors. Nancy Blacker writes, "Increased opportunities for training and education across the interagency through formal channels should lead to strengthened relationships that facilitate planners and decisionmakers at all levels of government. A focus on training and education should find its way through the jungles of personnel bureaucracy."[5]

Of course, with the expansion of any new and important field, government, military, and commercial organizations recognize the necessity for taming what can sometimes be viewed as a Wild West scenario in which there is no policy, guideline, or law. As Karen Dill argued, "The growth of the cyber domain continued while laws and policies to shape cyber security practice lagged due to a lack of knowledge gap within either a centralized government or private administration."[6] There has also been growing focus on cyber training across every cyber region



Associate research engineer Cassandra Stanfill, with Intelligence, Surveillance Augmentation, and Reconnaissance Branch, uses eye-tracking technology, among other methods, on test subject, Lieutenant Michael Emard, at Air Force Research Laboratory, Wright Patterson Air Force Base, Dayton, Ohio, July 21, 2016 (U.S. Air Force/J.M. Eddins, Jr.)

due to the recognition that cyber is a critical enabler of every aspect of JADO. This is of utmost importance within the joint military cyber enclave. DOD's main efforts in this area have largely focused on training cyber warriors, those highly specialized individuals with extensive technical training who can engage in the defensive cyber operations (DCO) and offensive cyber operations (OCO) vital to mission effectiveness. Training relates directly to highly specialized skills critical for accomplishing the tasks necessary for DCO and OCO. This is the cyber training wheelhouse, appropriately positioned for driving military cyber war.

Cyber Education. The word *education* carries with it several interesting connotations: *professional*, *strategic*, *nontechnical*, *leadership*, and *managerial*, to name a few. While many of these terms are definitive of the purpose and trajectory of education, this method of learning must not be pigeonholed any more than training. For instance, a common view is that education does not deal directly with technical problems and solutions, which may lead some to question its applicability within the cyber technical framework. However, this is a common misunderstanding currently being corrected through technically focused cyber career education within military and civilian institutions alike. For example, the Air Force Association CyberPatriot program "was well received by industry professionals and is now sponsored by multiple corporations including Northrop Grumman Foundation, Cisco, Symantec, and the University of Maryland University College."[7] Through programs such as CyberPatriot, technically savvy young women and men have their KSAs cultivated, eventually with the possibility of commissioning into a military service branch. Other governmental organizations are involved in the same types of workforce cultivation: "The National Security Agency (NSA) outreach to [science, technology, engineering, and mathematics] programs employed throughout the public school system and their National Centers of Academic Excellence in Cybersecurity serve as a foundation for curriculum development."[8] Other organizations are taking technical understanding to a more fundamental level. The U.S. Military Academy Mathematical Sciences Department is using mathematics education to "help prepare future military officers for leadership roles in the cyber-affected world in three tiers: (1) what all officers should know, (2) what highly technical officers should know, and (3) what cyber leaders should know."[9]

Such educational efforts are becoming more prevalent throughout military and civilian universities. This highly technical

focus belies the fact that cyber is a career field that not only crosses boundaries but is also filled with progressive challenges. With these challenges comes the need to educate and train personnel to a standard that includes a prismatic display of KSAs. This necessity has also highlighted the need to potentially use alternative methods of recruiting:

The cyber community has already acknowledged the idea that acquiring and developing the talent required for cyberspace operations may come from nontraditional sources or by nontraditional means. . . . The 2017 National Defense Authorization Act included a provision that allowed a pilot program for the direct commission of officers for cyberspace specialties.[10]

Through direct commissioning, the recognized gaps in the officer corps across DOD could effectively be filled in much the same way the specialty fields of medical doctors, chaplains, and lawyers are currently handled. This would allow civilians to enter the Armed Forces with increased rank, bonuses, and other incentives commensurate with opportunities, pay, and benefits offered in the corporate realm. Cyber talent is hard to come by, and direct commissioning is just one way to help with the critically undermanned force our military is currently experiencing.

Of course, technology is also a huge factor in education. Learning Management Systems, Student-Centered Active Learning Environments, and imbedded technologies within classrooms and across campuses are continuing to grow and advance. As highlighted in a RAND study of cyber learning as it relates to infrastructure operability:

Cyber learning relied on the fiber-optic network to deliver course content online to students throughout the region. Stakeholders reported that the fiber-optic network was the foundation for the program, without which students would not have been able to enroll, and that the network supported all student participation in cyber learning courses.[11]

Education is certainly a key to staffing and operating within cyberspace. Incorporating technology, alternative commissioning, advanced educational strategies, and technically focused education all play a role in assembling the JADO force necessary to ensure the Nation's security and dominance across the global cyber cosmos.

Cyber Training and Education Cross-Pollination. While training and education inhabit peculiar hemispheres within the cyber learning ecosystem, there is a natural and important wicking of concepts always present between the two. As stated aptly by Blacker, "When the opportunity arises to share or distribute expertise, each participating agency wins. Knowledge is gained and captured to spread around. Knowledge, if kept prisoner in its originating agency, will not contribute to the greater good."[12] Only through the sharing of the cyber challenges and lessons learned gathered by the training and education spheres can the advances and synthesis necessary for continued cyber progression take place. Spidalieri and McArdle claim:

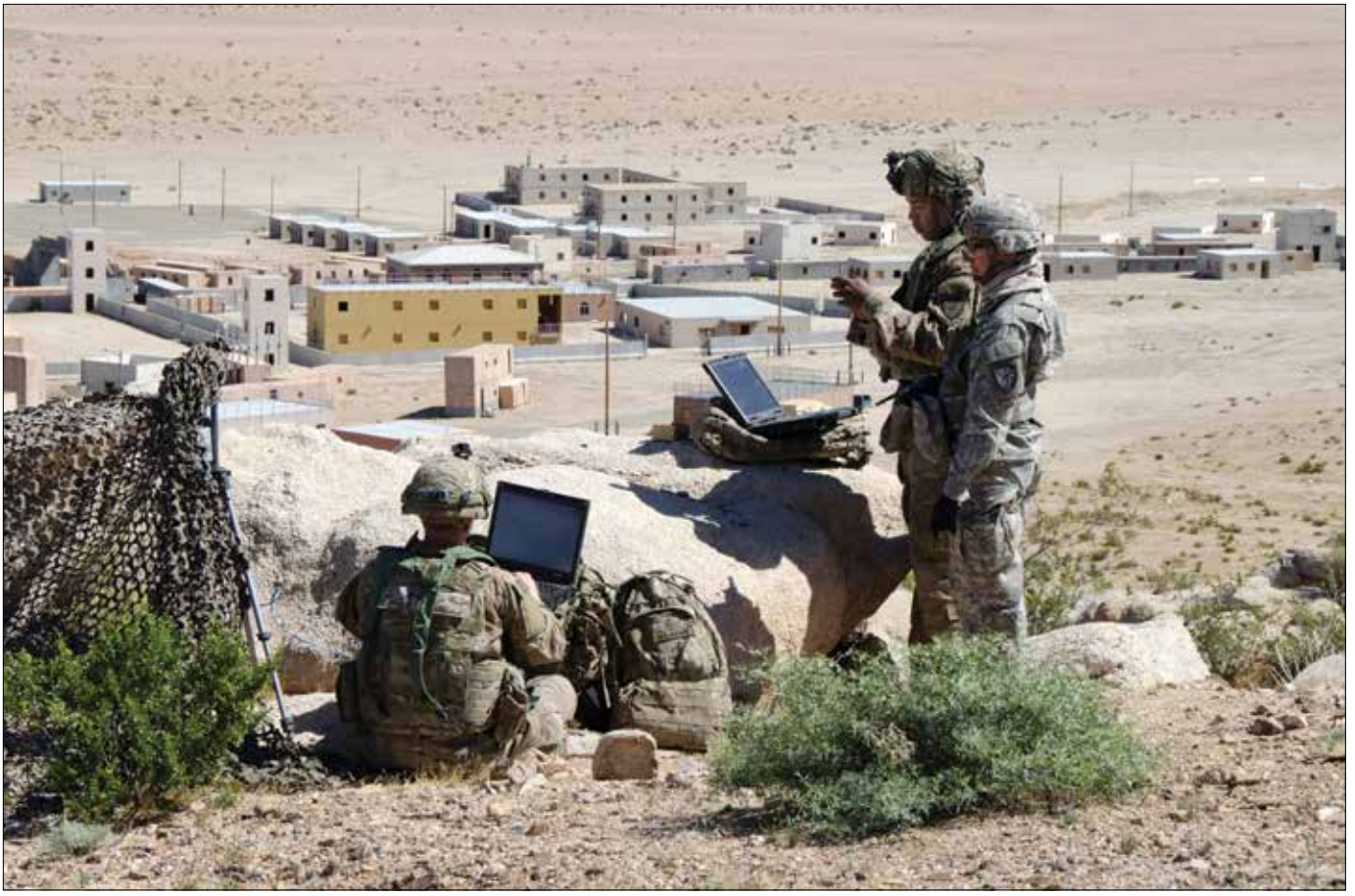
Cyber-strategic leadership . . . is not the same as, nor does it replace, the specific technical skills, knowledge, and abilities required to develop, administer, and defend the cyber environment. Rather it is a different and complimentary [sic] *set of skills, knowledge, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm*.[13]

Another bridging concept between training and education is the ability to transmit task-oriented learning alongside critical thinking. Without both present, the relationship shared between the learning and work environment will break down. Frank Katz writes, "In any educational setting, one of the great debates is whether a program of study provides both breadth and depth of knowledge in that curriculum."[14] While education is often seen as a method of delivering a breadth of information at a cost to depth, it is important to recognize the need to get "down in the weeds" in order to understand how cyber actions actually take place. This allows the leaders who emerge from educational programs to communicate intelligently and effectively with the technical force they have been tasked to lead. Conversely, technical students in training must be given the opportunity to understand strategic goals and objectives in order to comprehend how their discrete actions have lasting and deep impacts within the cyber strategic force construct and vision. Only through the complementary overlap between training and education will this beneficial relationship form and persist.

The IW Paradigm and IRCs

Although *IW* as a term and concept was broached in the 1990s, only recently has it returned with full force and promise as an established and mature organizational construct. As a result, CO and the training and education undergirding this capability have been perturbed and given a new mandate: interoperability with the ISR, EW, and IO disciplines. It is with this new perspective in mind that leaders, trainers, educators, and all the institutions surrounding them must proceed, bringing with them the responsibility of interleaving this impressive collection of IW capabilities and disciplines. An understanding of each discipline is necessary in order to see how they interrelate and combine within the IW superstructure. Trainers and educators can fix the focus and leadership of cyber warriors in the fusion and combinatory power expressed across these functions.

Cyber Operations. While the IRCs of ISR, EW, and IO have been available and in use for the better part of the 20th century and forward, cyber is the most nascent and is the capability that ties the rest of the IRCs together. This unusual placement of cyber operations in the company and annals of traditional IRCs makes cyber not only an intriguing field but also a veritable icon in its classification. When it comes to capability maturity, cyber is definitely a candidate, yet also an ever-growing IRC. This fact simultaneously makes cyber a powerful tool, a dangerous weapon, and an



Soldiers of 780th Military Intelligence Brigade set up cyber tools overlooking mock city of Razish at National Training Center, Fort Irwin, California, May 7, 2017 (U.S. Army/Bill Roche)

unbridled and sometimes wild beast. With this image in mind, we must understand the power of such a tool and how, as it ties the other IRCs together through networks, communications, and additional technological and infrastructure enablement, cyber is also a delicate and harrowing dynamo.

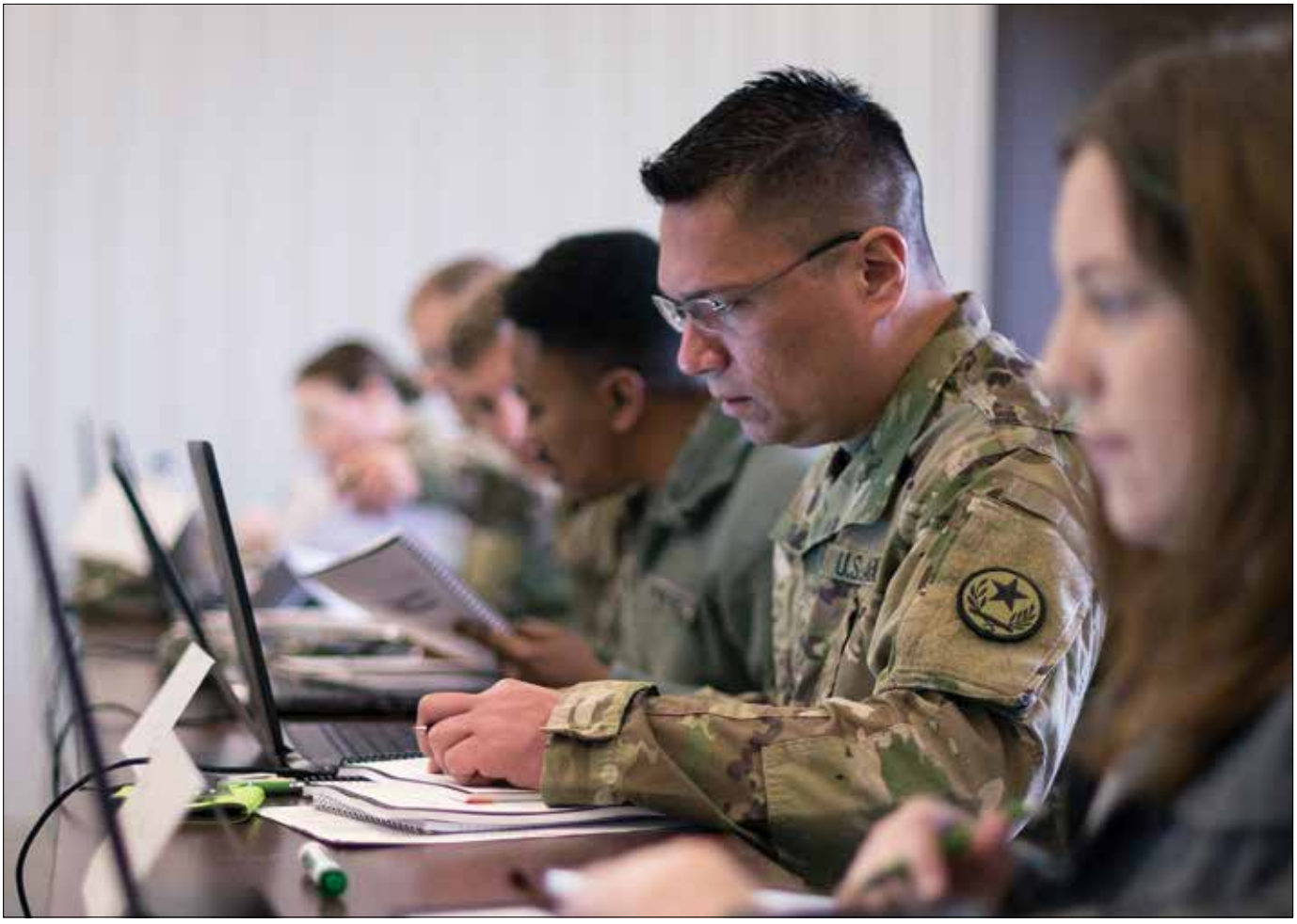
CO, especially in the U.S. stable of IRCs, is a capability unmatched by any other power in the world:

U.S. skills at cyberwar have no equal. U.S. institutions lead the world in the commercialized arts of persuasion, and the collection and analysis of personal information for commercial and political purposes have proceeded farther in the United States than anywhere else. No country is more advanced in digitizing and networking things.[15]

This supremacy is also relevant in relation to cyber capability across the spectrum of not only warfare but also industry, banking, and other critical infrastructure auspices. An article asserts:

The use of cyber assets has been a form of force projection that helps initiate crises far ahead of and beyond the frontlines, creating forms of more complex crises that affect energy infrastructure, banking systems, and political leadership, and not solely the Armed Forces fighting on the frontlines. Again, the extension of traditional military conflict is not a new strategy, but new technologies have been able to provide both the means and vulnerabilities to allow such operations at a scale not often witnessed before, and with a smaller investment in resources on the part of the aggressor.[16]

It is abundantly evident that cyber has wormed its way (pun intended) into basically every area of life, and it shows no sign of stopping. This is also evident in the fact that cyber has been established as a domain, specific to its own capabilities and effects within the greater military construct: "The allocation of 'domain' status to cyberspace (alongside maritime, land, air, and space) serves a bureaucratic purpose to ensure that CO receives sufficient financial and material support."[17] Overall, cyber has grown exponentially within its own sphere, reproducing itself like a virulent string into the nooks and crannies of practically all other areas of military strategy, operations, and training, techniques, and procedures. The cognitive effect from such rapid growth has been enormous, with *cyber* becoming not only a term on the tip of every tongue, but also a capability that every entity desires. Kamal Jabbour and Erich Devendorf claim, "Few cyber phenomena have captured the fascination of the media and the general public more than information theft through cyber exploitation and data exfiltration."[18] The terror and splendor inflicted on the collective considerations of the public show just



Texas Army National Guardsman analyzes network traffic as part of training week for exercise Cyber Shield 2019, at Camp Atterbury, Indiana, April 7, 2019 (U.S. Army/George B. Davis)

how powerful and mature cyber has become and just how much we have yet to learn.

Intelligence, Surveillance, and Reconnaissance. ISR is one of the oldest IRCs, with roots in warfare back to the dawn of recorded history. However, with the capabilities introduced in the 20th and 21st centuries, especially within the past two decades, ISR has become even more capable and powerful. As a discipline, there has never seemed to be any question concerning the power and necessity of ISR. This is evident in the amounts of money invested in IRC from the highest echelons of government, from organizations such as the NSA, Central Intelligence Agency, and Federal Bureau of Investigation, all of which depend on ISR operability and capability to function.

The great enabler in much of the maturation of ISR has been technology, again an area of obvious importance from the top down. With technology comes the need and desire to integrate other IRCs, most notably cyber capabilities, into the ISR capability framework. With this integration has come a new way of conducting ISR operations, including the kinds of information sought and the kinds of information environments accessed and used. After the breakdown of IW in the 1990s, ISR and the other silos of IRCs continued on parallel paths:

The ISR community kept building and operating systems of greater acuity and range. Electromagnetic warriors went back to mastering their magic in support of air operations, counter–improvised explosive devices, and other combat specialties. Psychological operators continued to refine the arts of persuasion and apply them to an increasing roster of disparate groups. Cyber warriors bounced through the space community before getting their own subunified command within which they could practice their craft.[19]

These paths have characterized the ways in which ISR has expanded its own sphere of operational influence and continued to add to this important and versatile IRC. Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs write:

A key component of such independent operability in both ISR and combat operations is the development and use of unmanned drones. The increasing use of drones for different functional areas (intelligence, electromagnetic countermeasures, direct strikes, etc.) and different operational environments (land, sea, air, amphibious) is an important consideration for flexibility in dynamic conflict situations.[20]

With key capabilities like drone and other network-dependent operations has come the inescapable tie-in of cyber, which has only served to abut ISR and cyber even more closely. With the merger of the Cyber 24th Numbered Air Force (NAF) and the ISR 25th NAF into a new 16th NAF, the objective is clear: a combined capability bringing with it not only cyber and ISR but also other IRCs into a combined IW capability.

ISR as a capability is also maturing across the globe:

Foreign intelligence services use cyber tools in information-gathering and espionage. Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities to enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power.[21]

With this idea in mind, it is important to see the advantages of such constructs and how the North Atlantic Treaty Organization (NATO) and the United States are going to meet the challenges of other nation-states and the capabilities they continue to develop. The maturation of ISR as a capability has kept pace with and even melded with cyber, leading to a continued technology and IRC arc that shows every sign of culminating in a combined IW construct.

Electromagnetic Warfare. As a shift and maturation of cyber and ISR capabilities has occurred, EW has followed a similar trajectory. As technology and cyber and ISR capabilities progress, EW as an IRC finds itself at a distinct advantage due to the peculiar niche it fills. EW is focused on controlling, disabling, and manipulating various signals and devices from and within multiple electromagnetic environments:

Electronic warfare can . . . be carried out by controlling devices that emit radio-frequency (RF) energy. New forms of RF signals pervade homes and cities: Bluetooth, Wi-Fi, 5G, keyless entry systems, and global positioning system, to name a few. The coming Internet of Things is essentially an Internet of RF-connected items. If software-defined radios (those capable of broadcasting or receiving signals over an arbitrarily selected frequency) become ubiquitous, they could be hijacked to jam or spoof targets hitherto inaccessible using traditional EW boxes.[22]

With this powerful reach into the RF spectrum, EW stands as an excellent cyber-enabled resource, capable of combining with other IRCs in many powerful ways. Other nations, such as China, have recognized this combination of capabilities for some time. For example, "A 2004 White Paper on National Defense increased the [People's Liberation Army] focus on 'informationalization' and advocated the use of cyber and electromagnetic warfare in the early stages of a conflict."[23] Under these circumstances and with a full understanding of the scope of these capabilities, it is in the distinct interest of NATO and the United States to hone their own capabilities in this realm while leveraging the full power of other IRCs. Again, Russia is already moving forward with this philosophy: "Russia has . . . developed multiple capabilities for information warfare, such as computer network operations, electromagnetic warfare, psychological operations, deception activities, and the weaponization of social media, to enhance its influence campaigns."[24] Not to be outdone, China has announced progress related to EW. In early writings, Major General Dai Qingmin anticipated operations involving "the destruction and control of the enemy's information infrastructure and strategic life blood, selecting key enemy targets, and launching effective network-electromagnetic attacks." He argued that this integration of cyber and electromagnetic warfare would be superior to the U.S. military's approach at the time of network-centric warfare.[25]

EW is another IRC that has existed for much of the 20th and 21st centuries. However, there has been a marked growth in capability with the advent of cyber and the continuing growth and expansion of ISR and IO that has led to a closer tracking of these capabilities, now seen from a holistic perspective. As these IRCs continue to cross streams and implement the others' precious proficiencies, the need for closer attention and support from NATO and the United States will be necessary.

Information Operations. IO is an IRC on par with ISR. IO looks at information in a way distinct from the other IRCs, however, especially as it relates to influence and the power of propaganda. NATO's Allied Joint Doctrine for Psychological Operations states that information operations are "coordinated and synchronized actions to create desired effects on the will, understanding, and capability of adversaries, potential adversaries, and North Atlantic Council approved audiences in support of the Alliance overall objectives by affecting their information, information-based processes, and systems while exploiting and protecting one's own."[26]

With the creation and proliferation of social media, IO has become a powerful tool in the world of cyber in general and ISR specifically. IO also draws power significantly from cyber as an enabling force. IO has been used for centuries as a way to influence, deter, and coerce through nonkinetic and generally nonlethal means: "Nonlethality and ambiguity, for their part, may be exploited to modulate the risk of reprisals—notably, violent reprisals—for having carried out information operations."[27]

This technique, combined with other nonlethal means such as cyber and EW, can generate power across the battlespace at many levels. China has used such integration and should be expected to continue this strategy into future conflicts in peace and in war. Elsa Kania and John Costello write, "The [PLA] Strategic Support Force's cyber corps approach the cyber domain in a much more comprehensive way, reflecting a highly integrated approach to information operations that actualizes critical concepts from PLA strategic and doctrinal approaches."[28] Other nations recognize the flexibility and power of IO as well as other advantages, including scalability, portability, cost, and ambiguity. For instance, "Russia recognizes that information operations offer an

opportunity to achieve a level of dominance . . . it provides a significantly less costly method of conducting operations since it replaces the need for conventional military forces."[29]

It is difficult not to see how powerful IO is in regard to influence and dominance since information has become and remains a key to everything from business to commerce to military operations, especially as it relates to social media:

Apart from its monetizing potential, social media has also become an excellent channel to mobilize support, disseminate narratives, wage information operations, or even coordinate military operations in the real world. States and non-state actors have started to extensively use social media to influence perception, beliefs, opinions and behaviors of their target audiences.[30]

The mature capability of IO across the globe and in and through organizational constructs lends itself well to the growth potential of IW, making it an undeniable asset in the combined scope of IW capabilities.

Recommendations and Conclusion

The mature capabilities manifested in and through CO, ISR, EW, and IO, respectively, tend to culminate in a combined IW merger that could harness and exploit all these competencies in myriad combinations. It is therefore incumbent on military and civilian training and educational institutions to keep pace with these changes. This is no easy task, especially considering the complexity of each IRC separately and then combining them in seemingly infinite ways. However, through its inherent professional and technical learning auspices, the IW construct can find purchase in the cosmic cyber intellectual domain.

While some schools have already begun to delve into interdisciplinary training and education regarding the IW IRCs, the integration of training and education regarding these capabilities and their interoperability must be further explored. This could be done through the introduction of curricula in a cross-disciplinary fashion to familiarize students with each capability while keeping their own discipline at the forefront. This will not only allow students the focus they need but also introduce them to how they and the other IRCs operate within the larger IW construct. Additionally, early exposure to the actual operational IW environment could be of special significance to students because this provides them a firsthand look at how these IRCs interleave and fuse together into a holistic product. Altogether, the confluence of IRCs, training, and education must combine into a structured JADO interdisciplinary construct unrivaled by our peer adversaries. JFQ

Notes

[1] Reginald Melton, "Developing Meaningful Links Between Higher Education and Training," *British Journal of Educational Studies* 43, no. 1 (1995), 43–56.

[2] Ibid.

[3] Burke Wilson et al., "Embedding Airmenship [*sic*] in the Cyberspace Domain: The First Few Steps of a Long Walk," *The Cyber Defense Review* 1, no. 1 (Spring 2016).

[4] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in U.S. Service Academies," *The Cyber Defense Review* 1, no. 1 (Spring 2016), 141–164.

[5] Nancy Blacker, "Winning the Cyberspace Long Game—Applying Collaboration and Education to Deepen the U.S. Bench," *The Cyber Defense Review* 2, no. 2 (Summer 2017), 21–32.

[6] Karen J. Dill, "Cybersecurity for the Nation: Workforce Development," *The Cyber Defense Review* 3, no. 2 (Summer 2018), 55–64.

[7] Ibid.

[8] Ibid.

[9] Andrew O. Hall and Brian M. Schultz, "Direct Commission for Cyberspace Specialties," *The Cyber Defense Review* 2, no. 2 (Summer 2017), 111–124.

[10] Chris Arney, Natalie Vanatta, and Thomas Nelson, "Cyber Education via Mathematical Education," *The Cyber Defense Review* 1, no. 2 (Summer 2016), 49–60.

[11] Andrea Phillips, Kun Yuan, and Shannah Tharp-Gilliam, "Performance of Cyber Learning," in *Evaluation of the Regional Choice Initiative* (Santa Monica, CA: RAND, 2016).

[12] Blacker, "Winning the Cyberspace Long Game."

[13] Spidalieri and McArdle, "Transforming the Next Generation of Military Leaders."

[14] Frank H. Katz, "Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models," *The Cyber Defense Review* 3, no. 2 (Summer 2018), 65–72.

[15] Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no. 1 (2017), 49–65.

[16] Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, "Hybrid War: High-Tech, Information and Cyber Conflicts," *Connections* 16, no. 2 (2017), 5–24.

[17] Christopher Argles, "A Conceptual Review of Cyber-Operations for the Royal Navy," *The Cyber Defense Review* 3, no. 3 (Fall 2018), 43–56.

[18] Kamal T. Jabbour and Erich Devendorf, "Cyber Threat Characterization," *The Cyber Defense Review* 2, no. 3 (Fall 2017), 79–94.

[19] Libicki, "The Convergence of Information Warfare."

[20] Danyk, Maliarchuk, and Briggs, "Hybrid War."

[21] Libicki, "The Convergence of Information Warfare."

[22] Jabbour and Devendorf, "Cyber Threat Characterization."

[23] Ibid.

[24] Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," *Strategic Studies Quarterly* 12, no. 3 (2018), 70–89.

[25] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018), 105–122.

[26] Allied Joint Publication 3.10.1(A), *Allied Joint Doctrine for Psychological Operations* (Brussels: North Atlantic Treaty Organization, October 2007).

[27] Libicki, "The Convergence of Information Warfare."

[28] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations."

[29] Ajir and Vailliant, "Russian Information Warfare."

[30] Bialy, "Social Media."