CEMA 2018 Hosts the Inaugural Electronic Warfare Cyber Convergence (EWC2) Workshop

By Dr. Jacob Cox and Colonel Dan Bennett, PhD

NOTE: This article provides a brief overview of outcomes obtained from the Electronic Warfare Cyber Convergence (EWC2) Workshop held in October 2018. The Army Cyber Institute plans to publish a full technical report addressing the results of the EWC2 workshop in its journal, "The Cyber Defense Review (CDR)" in early 2019.

The Army Cyber Institute (ACI) at West Point collaborated with the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S); Communications-Electronics Research, Development and Engineering Center (CERDEC); Association of Old Crows (AOC); Electronic Warfare Associates (EWA), and Soar Technology, Inc. to host its inaugural Electronic Warfare Cyber Convergence (EWC2) workshop in conjunction with the 2018 Cyberspace Electromagnetic Activities (CEMA) Conference, 23-25 October 2018. The workshop bookended the CEMA conference with the goal of identifying friction points, gaps, and research opportunities surrounding the Army's merger of Electronic Warfare (EW) and Cyber.

Prior to integration, these communities were largely separated and widely varied across the military services, particularly if you consider aspects of DOTmLPF-P (Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities, Policy). They represented a very stove-piped approach. However, other countries like Russia and China have taken a much more holistic approach in how they integrate capabilities in EW/Cyber, as well as in Signals Intelligence (SIGINT) and Information Operations (IO). Russia's skillful use of EW/Cyber/IO in the conflict with Ukraine proved particularly alarming, making it clear that future conflicts will require kinetic and non-kinetic maneuver, both physically and cognitively, across multiple domains. We can expect enemies to employ cyberspace attack capabilities (disruptive and destructive malware), EW capabilities (jamming and signal geolocation), and space capabilities that deny access to PNT (positioning, navigation, and timing), satellite communications, and other capabilities to deny U.S. Forces freedom of maneuver and tactical advantage. Adversaries may even attempt to strike at key homeland cyber physical installations to disrupt or delay deployment of forces or manipulate national commitment to potential or ongoing conflicts. These concerns are driving changes in the way the Army employs personnel, conducts operations, and resources technological capabilities.

The EWC2 workshop provided a collaborative environment for thought leaders, decision makers, innovators, and researchers across military services, defense agencies, and civilian organizations to discuss, debate, organize, and determine the friction points, hurdles, and ways forward within the converging EW and Cyberspace domains. More than 50 military, government, and industry personnel participated in multiple breakout sessions to identify doctrinal gaps, friction points, and innovative research needed to advance and support Cyberspace Electromagnetic Activities (CEMA) in a space that is increasingly congested and contested. The outcomes of this workshop focused on the next stage of EW/Cyber research objectives needed to enable friendly forces to operate effectively in current and future battlefields while deterring, denying, disrupting, countering, or destroying the adversary's ability to do the same.

The topic areas selected for this workshop included: (1) Identification of EW/Cyber friction points, (2) How to build the EW/Cyber workforce, (3) Operational employment of EW/Cyber capabilities, (4) Employment of artificial intelligence (AI) in EW/Cyber operations, and (5) Leveraging EW/Cyber for IO. Participants were challenged to develop questions pertaining to gaps, friction points, and research opportunities for each of these topics to drive future discussions by leadership and researchers on how to close the gaps, alleviate friction, and address research opportunities.

Friction Points. During the workshop, participants noted that the Army's convergence campaign has the potential to erode understanding that EW and Cyber are at their core separate and distinct capabilities with unique considerations for employment. For instance, electronic warfare seeks to preserve the electromagnetic spectrum for friendly use while denying its use to the enemy. Cyberspace operations employs cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace.[1] The electromagnetic spectrum is a physical medium for cyberspace operations. EW can be employed as a standalone capability, or it can serve to provide access for Cyberspace capabilities. Elements of EW include electronic attack (EA), electronic warfare support (ES), and electronic protection (EP). Cyberspace operations include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoD information network operations (DoDINO).

The convergence of these two capabilities provides for Cyberspace Electromagnetic Activities, which are activities leveraged to seize, retain, and exploit an advantage over adversaries in both Cyberspace and the electromagnetic operational environment (EMOE), while simultaneously protecting the mission command system and denying and degrading our enemies' use of the same.[2] Convergence creates opportunities for Cyber and EW to overlap; however, convergence also creates potential for training, resourcing, and employment changes to dilute skills currently inherent in the EW and Cyber workforce as well as resources. After all, an EW operator and a Cyberspace operator, at their lowest levels, are not the same, and we cannot treat them the same. A similar analogy exists with artillery and armor soldiers. Even though they both operate machines (e.g. howitzers and tanks) delivering kinetic effects, they are not the same, and that is reflected in their training. Others have noted the potential impact to resources. In 2016, then Major Michael Senft (USA), argued that that the convergence of Cyber and EW would further limit the resources already allocated for EW.[3] Primarily, Senft argued that EW is only used in continuum of military operations[4] during Phase 2, "Seize the Initiative", while Cyberspace operations is used during all phases of military operations. As a result, concern over resourcing remains an issue. Hence, participants asked how resource allocation can be balanced in such a way as to not further constrain EW capabilities?

Personnel. As of October 2018, electronic warfare officers (EWOs) are branched Cyber despite not having received adequate Cyberspace operations training. This lack of training drove the personnel breakout group at the EWC2 workshop to ask what training is currently available or could be made available to qualify 17E, 18x or other MOS individuals to conduct Cyberspace operations organically. One participant put it this way:

[1] Joint Publication (JP) 3-0

[2] Army Doctrine Reference Publication (ADRP) 3-0

[3] Senft, M. "Convergence of Cyberspace Operations and Electronic Warfare Effects." The Cyber Defense Review. January 4, 2016.

[4] Joint Chiefs of Staff. 2001. Doctrine for Joint Operations, Joint Publication 3-0, Washington, D.C., September 10, pp. III-19-III-21.

> *With the bulk of 17As going to the Cyber National Mission Force to support Army and US CYBERCOM, the bulk of Cyber operations planning for FORSCOM is in the hands of the 17B. As a result, mission planning that goes on to request joint Cyber effects and enable the use of Cyber teams for the Brigade Combat Team (BCT) will reside in the 17B community (EWOs). With that in mind, what cross training is needed for 17As and 17Bs to synergize effects on the battlefield?*

Participants also identified the Force Design Update (FDU) as a potential gap in future operations; the question being whether the current FDU can support prolonged 24/7 operations? Similarly, participants considered what the integrated CEMA Cell will look like in 2025? Whatever that is, participants believe it will have to integrate IO, SIGINT, space operations, and other Information Related Capabilities (IRC) as well.

Another gap this group considered focused on mission essential task lists (METL). The Army has a motto of "train as you fight"; however, methods for identifying and developing EW/Cyber tasks based on innovations occurring in the field do not currently exist. It is indeed encouraging that we have operators who are capable of innovating in the field; however, there are currently no METL tasks for EW at Corps or below. Funding is inherently tied to METL. Therefore, a doctrinal question is what tasks need to be incorporated into unit METL for Strategic units down to the Tactical units to ensure EW/Cyber operations are addressed during training exercises?

Operations. The discussion over operational employment of EW/Cyber capabilities touched upon intelligence, doctrine, and understanding of capabilities, i.e., there appears to be a gap in the speed with which actionable intelligence from classified sources can be extracted and shared with warfighters. The question posed is how can U.S. Military forces expedite this process? Another identified gap is the lack of tools to create access, perform collection, or generate effects in support of Cyberspace operations. This discussion produced two questions. First, what tools are already developed and available to support tactical Cyberspace operations for Division - Brigade Combat Teams (DIV-BCTs)? Second, what processes exist or could be created to rapidly validate existing open source tools for use? Some participants stated there is a lack of authority to conduct EW/Cyber training and operations. Their perception being that very few leaders, lawyers and legislators are currently competent in EW/Cyber law, policy and operations. This potentially prevents requests from being generated and staffed at Divisions and Brigades. These education gaps also concern both General Mark Milley and Senator Mike Rounds (R-SD), who spoke on the issue at ACI's International Conference on Cyber Conflict (CyCon) U.S., 2017.

Artificial Intelligence. During TechNet 2018, Colonel Steven Rehn, TRADOC Capability Manager (TCM) for Cyber at Ft Gordon, GA, highlighted several areas where artificial intelligence (AI) can aid EW/Cyber capabilities. For instance, the application of AI could help reduce the time needed for EW/Cyber systems to reconfigure and change techniques (or tools) to enable and protect friendly forces' access to spectrum and information systems while denying adversaries access to the same.

AI could do this by integrating into EW/Cyber systems and quickening their observe, orient, decide, and act (OODA) loop well beyond human capabilities. AI could also enable and enhance dynamic planning and execution, dynamically identify threats, close the gap between technology and operator capabilities, and minimize focus on data analysis to enable a shift to execution. Rehn further added there is a need to apply AI to Cyberspace Modeling and Simulation (M&S) and Advanced Analytics (e.g. risks/opportunities and actions/effects), and to dynamically reshape Cyberspace (e.g. platforms, networks, runtime environments, software, and data).

Many service members, however, struggle to understand what AI is and what it isn't. In general, AI can be considered as a concept for improving the performance of automated systems for complex tasks.[5] Today these tasks include perception (sound and image processing), reasoning (problem solving), knowledge representation (modelling), planning (strategy and action sequences), communication (language processing), and autonomous systems (robotics).[6] Additionally, as Trent and Lathrop point out, what is considered AI today may not be considered "intelligent" tomorrow, e.g. in the 1980s, a grammar checker seemed intelligent; however, such algorithms are ubiquitous in today's word processing software.

As to the application of AI to enhance EW/Cyber capabilities, participants asked that leaders and researchers consider which systems and platforms in current use could benefit from automation. Participants also noted that humans may place too high an expectation on autonomous systems to perform flawlessly. They noted that humans frequently fail to perform perfectly; yet autonomous systems seem to be held to a higher standard. These observations drove some interesting questions. First, what level of error threshold are we willing to accept from systems working autonomously? Second, assuming we can't account for all the data a system is evaluating in real-time when it makes an error, who gets blamed for the error when it occurs?

Information Operations. As defined in Field Manual (FM) 3-13, "*Information operations (IO) creates effects in and through the information environment. IO optimizes the information element of combat power and supports and enhances all other elements in order to gain an operational advantage over an enemy or adversary. These effects are intended to influence, disrupt, corrupt or usurp enemy or adversary decision making and everything that enables it, while enabling and protecting friendly decision making. Because IO's central focus is affecting decision making and, by extension, the will to fight, commanders personally ensure IO is integrated into operations from the start*."

The very definition of IO led to the first question asked by the group: how do we provide lead time for EW/Cyber capabilities (non-kinetic) into kill chains that typically terminate with kinetic effect given the mismatch in timing and tempo of EW, Cyber, Space, and IO? Another question offered was how do we accelerate the tempo of planning and deploying EW/Cyber effects through any means? Additionally, the group asked how will U.S. Forces perform battle damage assessment (BDA), and what will be the battle damage indicators—measures of performance (MOP) and measures of effectiveness (MOE) across EW, Cyber, Space, and IO – when EW/Cyber capabilities are applied?

While the initial focus of the EWC2 workshop was the convergence of EW and Cyberspace operations, additional identified friction points include those among EW, Cyber, IO, Intel, Space, and Signal. Fortunately, the Army is already conducting a study to ascertain how all of this might fit under the umbrella of *Information Warfare Operations*. One participant referred to the current environment as more of a circus tent—hinting at how these disparate disciplines must learn to complement one another rather than trying to figure out how to integrate all of them. Many elements of the U.S. Army and joint

[5] Trent, S. and Lathrop, S. "A Primer on Artificial Intelligence for Military Leaders". Small Wars Journal. Aug 23, 2018.

[6] Ibid

forces must work together and address these friction points, gaps, and research challenges to create synergy in our fighting force and ensure dominance in future conflicts involving multi-domain battle. Furthermore, with near-peer adversaries investing in, and building, their EW and SIGINT capabilities, the United States must quickly grasp these issues and address them to build superior capabilities at speed. The U.S. Army's definition and understanding of Information Warfare Operations (Figure 1) must also be resolved, and that will be further discussed in the technical report being released by ACI in early 2019.

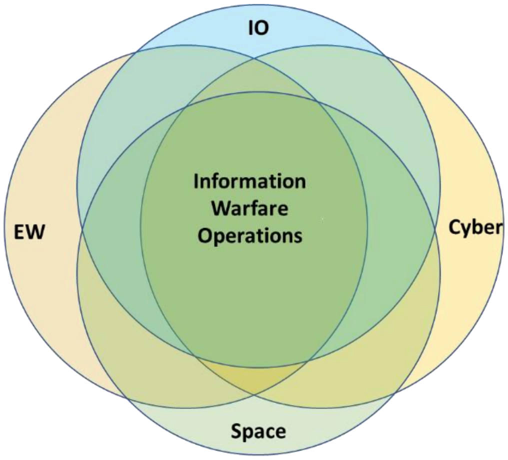

Figure 1. Information Warfare Operations

About the authors: Dr. Jacob Cox is a retired Army Major and research scientist with Soar Technology, Inc., an artificial intelligence research company, and Colonel Daniel Bennett, Ph.D. is the Director of Research at the Army Cyber Institute at West Point.