The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence

Major (Ret.) Jacob Cox, Ph.D.
Colonel Daniel Bennett, Ph.D.
Colonel (Ret.) Scott Lathrop, Ph.D.
Lieutenant Colonel (Ret.) Chris Walls
Chief Warrant Officer 4 (Ret.) Jason LaClair
Lieutenant Colonel Clint Tracy
Chief Warrant Officer 4 Judy Esquibel

ABSTRACT

With Electronic Warfare joining the Cyber Branch in October 2018, numerous opportunities and challenges that affect warfighters are surfacing. To capture and consolidate some of these observations, the Electronic Warfare Cyber Convergence (EWC2) workshop, held in conjunction with the 2018 Cyberspace Electromagnetic Activities (CEMA) conference, provided an opportunity for experts from military, government, commercial and academic backgrounds to compare insights, explore friction points, consider deeper issues and note potential research opportunities within the EWC2. In this workshop, participants learned that the convergence of EW and cyberspace operations is only the initial step towards the greater goal of controlling information on the battlefield.

I. INTRODUCTION

On October 1, 2018, the United States Army merged its electronic warfare (EW) functional area into its Cyber Branch. This merger supports the Army's doctrinal requirement to perform cyberspace and EW operations in support of unified land operations and joint operations.[1] As with any merger, however, friction points involving culture, policy, doctrine, operations, and technology can create obstacles to achieving a cohesive organization. To address these challenges, the U.S. Army must identify and address the merger's shortfalls across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P). The desire to address these shortfalls was at the forefront of the inaugural Electronic Warfare Cyber Convergence (EWC2) Workshop, which was organized and moderated by the Army Cyber Institute (ACI) and industry volunteers in collaboration with the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S), Communications-Electronics Research, Development and Engineering Center (CERDEC),[2] and the Association of Old Crows (AOC).

During the workshop's two-day event, leaders, operators, and researchers across military services, defense agencies, and civilian organizations discussed, debated, and identified friction points, hurdles, and ways forward within the converging EW and Cyber communities. Workshop focus areas included innovative research, training, and opportunities to advance and support CEMA.[3] Participants also explored how to leverage this convergence to allow commanders to outmaneuver adversaries, both physically and cognitively, in multi-domain battle. Products of this event included a consolidated set of friction points and challenges facing EW and Cyber convergence along with suggestions and opportunities for enabling friendly forces to operate effectively in the current and future battlefield. Moreover, participants focused on how to seamlessly achieve these goals for warfighters who ultimately care about how cyberspace and EW operations will enable them to gain dominance in multi-domain battle and win.

The topics of this workshop evolved from a discussion of friction points that were created with the convergence of EW and Cyber. The ACI encouraged exploration of operational and personnel gaps; and the link between EW and cyberspace operations and information operations (IO). Technological challenges discussed at TechNet 2018 contributed to the selection of machine learning (ML) and artificial intelligence (AI) as enablers for cyberspace and EW operations. These topics led to the workshop's five focused areas: 1) general friction points of EW/Cyber convergence; 2) employment of EW/Cyber personnel; 3) operational employment of EW/Cyber capabilities; 4) employment of AI/ML in cyberspace and EW operations; and 5) leveraging CEMA for IO. Each participant was assigned two topic areas based on experience, expertise, and interest. Participants rotated between focus areas on both days of the workshop. As a result, the participants generated vibrant discussions on directions, trends, and challenges of EW/Cyber convergence and were challenged to develop questions about gaps, friction points, and research opportunities for each of these topics. These discussions also led participants to acknowledge that greater convergence is yet to come as more areas of expertise fall under information warfare operations. This report summarizes the workshop's outcomes, which will ideally serve to drive future discussions by leadership and researchers to close gaps, smooth friction points (perceived or not), and pursue research opportunities to improve cyberspace and EW operations.

II. BACKGROUND

Before convergence, EW and Cyber communities were largely separated and widely varied across the military services in terms of equipment, unit organization, operational tasks, and culture. Meanwhile, near-peer adversaries have demonstrated integrated EW and cyberspace capabilities along with Signals Intelligence (SIGINT) and Information Operations (IO) capabilities in real-world operations. Russia's use of EW/Cyber/SIGINT/IO[4] during its conflict with Ukraine, and in Syria, proved particularly illuminating—indicating future conflicts will require kinetic and non-kinetic maneuver, both physically and cognitively, across multiple domains.[5] For instance, adversaries may attempt to strike at homeland installations via kinetic and non-kinetic means to disrupt or delay deployment of forces, manipulate national commitment to potential or ongoing conflicts, or disrupt the warfighting functions of deployed units.

We now expect our enemies to employ cyberspace attack capabilities (such as disruptive and destructive malware); EW capabilities (jamming and signal geolocation), and space capabilities that obstruct satellite use to disrupt U.S. military communications; positioning, navigation, and timing (PNT); synchronization; and freedom of maneuver. These threats make it clear—if the U.S. military is to succeed in this future battlespace, it must gain combat superiority over its adversaries by defending its information networks in cyberspace and securing unimpeded access to the electromagnetic spectrum (EMS) while denying its adversaries the ability to do the same.

These concerns are driving the Army to challenge the way it employs personnel, conducts operations and focuses on technological capabilities. In response, the EWC2 workshop provided a collaborative environment for participants to discuss, debate, organize and determine the friction points, hurdles, and ways forward within the converging EW and Cyber communities. During multiple breakout sessions, participants attempted to identify friction points, doctrinal gaps, and innovative research needed to advance and support cyberspace and EW operations. Hence, the workshop's outcomes focused on the next stage of technical and non-technical objectives needed to enable friendly forces to operate effectively in current and future multi-domain battlefields while deterring the adversary's ability to do the same.

III. GENERAL EW/CYBER FRICTION POINTS

Mergers frequently struggle with a clash of personalities, cultures, priorities, and leadership that creates points of friction or resistance to a unified application of effort. For instance, during the workshop, one participant expressed concern that there is a potential for the Army's EW/Cyber convergence campaign to erode the fundamental understanding that cyberspace operations and EW operations are at their core separate and distinct capabilities with unique pros and cons. For instance, EW seeks to preserve the EMS for friendly use while denying its use to the enemy. Subdivisions of EW include electronic attack (EA), EW support (ES), and electronic defense (ED)[6] Cyberspace operations (CO) include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoD information network (DODIN) operations. Cyberspace operations employ cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace,[7] which admittedly depends on the EMS at the physical communication layer. However, these two capabilities have different focuses, requiring different high-demand, low-density skill sets.

By merging EW and cyberspace capabilities, the U.S. Army hopes to achieve better coordination across the EMS and cyberspace to gain advantage over its adversaries. The potential to dilute skills and training resources that are already inherent in EW and cyberspace workforces does exist. In 2016, Senft stated that the convergence of Cyber and EW would further degrade the already limited resources allocated for EW.[8] He argued that EW is only used in the continuum of military operations during Phase 2, "Seize the Initiative," while cyberspace capabilities are employed during all phases of military operations causing it to receive more attention and resources. Arguably, EW has a role during other phases, but Senft's point raises a valid concern that resourcing remains an issue across training, equipping, and staffing. Hence, participants asked how the Army can better allocate resources without further constraining EW capabilities?

Participants noted that current friction points mostly reside in the acquisition, policy/authorities, classification boundaries, and force structure. Much work is needed to balance requirements with system acquisition processes to ensure better vendor engagement. Policy/authorities were the most contentious of the friction points listed above. The majority of working group members view policy/authorities as a hindrance to mission accomplishment. However, working group members noted that it is not necessarily policies per se, that are the problem, but rather the interpretation of the policies at the strategic and operational level that falls short. This happens when there is a lack of technical understanding required to accurately and quickly validate a tactical course of action (COA). Maturing of the force and additional training for personnel working at the strategic and operational level will help in this regard. From a classification standpoint, participants expressed frustration at the lack of cross-domain solutions available for sharing operationally relevant data with warfighters. If commanders and staff are to gain the advantage over adversaries in multi-domain battle, the Army must pursue a national-level forcing function to ensure they receive relevant information promptly.

IV. EMPLOYMENT OF EW/CYBER PERSONNEL

The Army has taken great strides towards increasing its capability to conduct EW and cyberspace operations. The initial focus was on staff-level manning with the creation of the CEMA sections as the staff focal point for planning, integration, and synchronization of EW and cyberspace operations. These staff elements are expected to be organic at each echelon from the Brigade headquarters to Theater Army, and they are staffed with existing EW and Spectrum Management Officer (SMO) personnel, plus some limited new personnel authorizations. Unfortunately, these members have received limited or no training on their new requirements. Moreover, the lack of EW equipment resulted in limited training on the actual conduct of EW operations. Similar SMO training primarily focuses on the administrative tasks of spectrum planning and deconfliction rather than spectrum maneuver. As a result, a major overhaul of training is required to enable the CEMA section to perform as designed. CEMA Section personnel need to be experts in EW systems with a strong grasp of existing cyberspace capabilities. Additionally, SMO personnel must be trained to advise the CEMA section on the best employment of its assigned capabilities based on the EMS and physical terrain aspects of the operating environment and to help mitigate the unintended effects of employed systems. In addition to individual and collective training at the tactical level, the CEMA section also requires classified intelligence and reach-back support to EW and cyberspace subject matter experts to help it address emerging threats in a rapidly changing environment. This reach-back support would help fill training and expertise gaps and could potentially be offered by future formations such as the recently approved Cyber Warfare Support Battalion (CWSB).

The CEMA section also struggles with limited intelligence support. As the Army grows its EW and cyberspace forces, there has been little or no corresponding growth in the supporting intelligence formations. EW and cyberspace operations require specialized technical and timely intelligence as well as the analysis and characterization of collected signals. There is significant work required to shape future operating environments through detailed intelligence preparation of the battlefield (IPB). IPB to support EW and cyberspace operations requires that the electromagnetic and cyberspace environment be baselined along with capabilities to support situational understanding. Electronic Intelligence (ELINT) surveys are required to identify and characterize signals of interest and develop signatures before a conflict to enable EW systems to rapidly identify and target signal and associated adversary units in the opening phases of future conflicts. Current intelligence forces have already struggled to meet existing intelligence requirements before the surge in EW and cyberspace forces and capabilities. The Army will need to expand its intelligence operations in Phase 0 to gather the necessary intelligence and information to enable emerging EW and cyberspace capabilities. In an era of limited resources and numerous critical gaps across the Army, any increase in intelligence capability has not been a high enough priority to be resourced.

To further exacerbate the lack of intelligence, and due to the cross-domain deficiency discussed in the previousection, CEMA sections struggle to receive and share SIGINT and other highly classified information with other associated intelligence elements. The CEMA section, like the rest of their associated headquarters, operates on SECRET networks while their much-needed intelligence support, such as SIGINT, is resident on TOP SECRET networks. CEMA personnel are not currently mandated to receive the level of clearance necessary to receive and work with this information. To integrate with the Mission Command systems on SIPR, current and future EW systems are only required to operate at the SECRET level, which places policy and technological barriers that degrade the effectiveness of current and future capabilities. The lack of cross-domain solutions further exacerbates the exchange of needed information.

The CEMA Cell of the future may also look different than today. The function may end up absorbed into another staff element such as the fires section or a future information warfare section. Regardless of any potential reorganization, the requirements to understand and integrate EW and cyberspace capabilities into operations will remain. The CEMA Cell of the future will have to overcome current issues with sharing classified intelligence with the CEMA Cell being able to access TOP SECRET information needed to plan, integrate, and synchronize EW and cyberspace effects. A fused picture that integrates not only EW and cyberspace information, but also SIGINT, Space, and IO reflecting the latest information and intelligence, must be available to our planners. This capability may look more like the design for the coming Intelligence Cyberspace Electronic Warfare Space (ICEWS) detachment that is a part of the future Multi-Domain Task Force (MDTF). The Army has already identified requirements to invest in a common operating environment (COE) with its command post computing environment (CPCE) that attempts to address these challenges. However, these programs are only in their nascent stages, and much work and research are needed to bring the analytics and tools to bear that will provide commanders and staff with situational understanding. Future CEMA sections must also be experts in utilizing assigned sensors (EW, Cyberspace, Space, and intelligence), intelligence resources, open source information, and battlefield innovation to see and understand their operating environment and to conduct planning to integrate EW and cyberspace capabilities into every operation to provide targeting options and defend their unit's networks and systems. These capabilities should be the basis of collective training for the CEMA section.

Evolving EW Platoons and Training

As EW platoons are fielded with equipment and capabilities, it becomes critically important to establish common training standards. Like other specialties, the EW Platoons should have both collective and individual task standards that will allow their leaders to establish training plans and determine their unit's readiness for its wartime mission. Today, units are using their initiative to establish their tasks and standards. These tasks and standards need to be passed to Training and Doctrine Command (TRADOC), so they can be normalized and codified into Army tasks and standards. These tasks and standards should be maintained, with the advice and consent of Army Cyber Command (ARCYBER) as the operational headquarters for all EW and cyberspace forces in the Army, at the Cyber Center of Excellence, an arm of TRADOC.

The newly approved EW platoons at the Brigade level (EW Company at Corps echelon) will work with sensitive equipment that if used improperly could have adverse effects on U.S. Forces, allies, and non-combatants. To ensure that these capabilities are employed correctly, each of the operators should be certified on their assigned equipment. As the Army begins to operationalize tactical cyberspace operations, these units may receive new capabilities in an ad hoc manner. Platoons should look to the mechanized and armor formations and consider using a Master Gunner who is responsible for certifying each of the soldiers on their assigned equipment. New EW/cyberspace capabilities could then be passed through the Master Gunner who would assume responsibility for training the rest of the operators in the platoon. Hence, the Master Gunner would require extensive training both as a cyberspace operator and EW expert. This role is ideally suited for a warrant officer.

In the EW and Cyberspace mission areas, warrant officers are the technical subject matter experts, and they have a training and development track to enable them to fill this role. This makes the warrant officer a key participant of CEMA sections at all echelons as integral to advising the CEMA chief and the commander on the capability and employment of assigned systems. Despite the recognition of their key role, participants noted that warrant officers were left off the EW Platoon's force design. This gap potentially leaves a critical vulnerability in our forward most units of action.

METs and Readiness

In the Army, a unit's readiness is directly linked to its mission essential tasks (METs). These tasks are the priority for unit training and are typically tracked by commanders. For EW and cyberspace operations to receive the necessary training support, their associated tasks must be included in (or directly influence) the accomplishment of its MET for maneuver formations from battalion to division level. METs are critical as they affect the Objective Task evaluation of a unit's readiness to accomplish its wartime mission. Without this emphasis, unit's will not assign EW and cyberspace operations training the priority required to match peer adversaries.

Emphasis on the importance of EW and cyberspace training must be top-down and heavily integrated. The U.S. Army's Cyber Directorate in the Army G3/5/7 (Operations, Planning and Training section), DAMO-CY, is responsible for developing the Army EW and cyberspace strategy and is uniquely able to orchestrate the integration of all aspects of the man, train, and equip mission into Army foundational documents that will ultimately drive requirements, resourcing, and prioritization. Guidance from these strategies will be amplified through other foundational Army training documents such as the U.S. Army Forces Command (FORSCOM) Training Guidance. This guidance is published annually and serves as the basis from which all Army units develop their priorities for training. The continued requirement to address CEMA in annual training guidance would influence commanders to increase their priority for EW and cyberspace training.

Army exercises also provide an opportunity to increase training emphasis for EW and cyberspace operations. Combat Training Centers have been used to exercise limited EW and Cyberspace capabilities. Unfortunately, these tasks have not been prioritized as critical tasks. When used, Opposing Force (OPFOR) capabilities have seen limited or constrained use due to concerns that it will degrade the unit's networks or systems to the point that it is prevented from achieving its training objectives. Also, EW and cyberspace topics are rarely—if ever—topics of conversation in the commander's end-of-rotation After Action Reviews (AAR). Instead, it is relegated to other AARs not typically attended by commanders. To increase the visibility and importance of EW and cyberspace in the eyes of commanders, the Division Trainer—who is responsible for shaping a Combat Training Center (CTC) rotation—can state that EW and cyberspace operations will be a primary objective for the rotation, which would ensure the rotational Commander's attention and their inclusion in mid-and end-of-rotation AARs. Broader employment of OPFOR EW and cyberspace capabilities would also demonstrate a more realistic threat picture and would likely serve as an eye-opener to how vulnerable forces are to the EW and cyberspace threat. All of these taken together would be a powerful message on the increased importance of EW and cyberspace operations, especially if the message is tied to maneuver.

Cyber and EW communities have primarily addressed cyberspace and EW operations as technical issues, not operational ones. However, to best address the U.S. military's personnel, equipment, and training challenges, a different perspective is needed. Instead of viewing operations through the lens of cyberspace and EW (or even Intelligence, Mission Command, or Fires), leaders need to consider these capabilities through the lens of the maneuver commander. This viewpoint will enable changes in how the U.S. Army approaches these challenges, and it will allow warfighters to effectively integrate cyberspace and EW capabilities into military operations—helping warfighters visualize, describe, and direct operations in the EMS and cyberspace.[9]

Recruiting and Retention

The emerging technological advances in EW and cyberspace capabilities require a more technically-skilled Soldier. The Army has begun to address this challenge through assessing and adjusting basic test scores to qualify Soldiers for these more technical military occupation skills. One challenge is that the type of individuals that are required to perform these missions are inherently sought after in the public workplace, and their value and job opportunities only increase as they receive advanced training in the service. These facts create challenges for recruiting and retaining these soldiers. Several ideas such as monetary bonuses, advanced schooling, assignment stability, and flexible standards on physical fitness and uniform requirements were discussed. While monetary bonuses can help to recruit initial personnel and early bonuses tied to utilization tours could help keep them longer, it is hard for the military to compete with salaries offered in the corporate workplace.

While flexible standards on physical fitness, uniform, and other military standards may sound good at face value, the opinion of the working group was that anything that undermines the military's discipline and sense of mission, which creates camaraderie within the service would do more harm than good by retaining the wrong type of personnel. Similarly, personnel solely motivated by monetary inducements may not have the right motivations necessary to integrate into Army formations successfully. Working group participants suggested that the best personnel are the ones that share the sense of mission and purpose. Furthermore, benefits that help personnel perform their jobs better, such as longer assignment periods, advanced schooling, and the ability to focus and professionalize in specific mission areas are options worth pursuing. However, this is an area deserving of greater investigation and analysis.

Officer Development

In the new design for EW platoons, a Career Mission Field (CMF) 17 (Cyberspace Warfare) Second Lieutenant is the platoon leader. EWC2 participants questioned whether newly commissioned officers are the ideal candidate for the role. After all, the EW Platoon is a Brigade, not a company, asset. Are lieutenants expected to possess the technical savvy and operational understanding needed to facilitate the employment of EW capabilities? Like other mission areas, lieutenants will likely be responsible for the leadership and operational employment of their platoons and will lean on their non-commissioned officers (NCO) and a warrant officer (if included in the future force design) for technical advice. These officers will receive the same training as an officer destined for service within the Cyber Mission Forces (CMF), but with additional training of EW.

Participants asked whether these officers would benefit from more diversified career paths that include time leading in tactical as well as operational and strategic units. Officers who serve in tactical roles can serve as ambassadors able to translate the highly technical aspects of EW and cyberspace operations into maneuver language that resonates with battlefield commanders. This position also affects the broader Army's perception of EW and cyberspace forces as platoon leaders will serve as the primary point of contact to U.S. military leaders. An argument can also be made that these officers should be the best of the CMF 17 to assist in the adoption and integration of this emerging capability.

V. OPERATIONAL EMPLOYMENT OF EW/CYBER CAPABILITIES

The operational employment of EW/Cyberspace capabilities touched upon intelligence, doctrine, and understanding of capabilities. These gaps stretch across how warfighters receive cross-domain intelligence, apply cyber/EW capabilities and understand the impact of cyberspace and EW operations on their warfighting functions. For instance, there is a gap in the timeliness in which actionable intelligence is extracted from classified sources and shared with warfighters. Participants identified the need to identify a cross-domain solution that can expedite this process. Understanding the impact of cyberspace and EW operations was also identified as a key weakness for commanders and staff. With regard to understanding the impacts of cyberspace and EW operations on the battlefield, EWC2 participants observed that leaders from Brigade through Division struggle to obtain an adequate understanding of what tasks EW and cyberspace operations can perform. They also lack information about what tools/assets are arrayed to perform these tasks—both within the Army and the broader Joint force. In the Army's Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EW CBA), published in 2013, Cyber Situational Awareness [Understanding] was listed as the number one gap within its Functional Needs Assessment (FNA) Gaps with Doctrine Aspects.[10] Six years later, our research demonstrates this remains a gap in U.S. Army capabilities.

Participants also identified the lack of tools to create, access, or perform collection and effects in support of cyberspace operations as a gap. This discussion developed along two lines. First, what tools are already developed and available to support tactical (BCT-DIV) cyber? Second, what processes exist (or could be created) to rapidly validate existing open source tools for use?

The Army has embraced events like Cyber Quest and Cyber Blitz to help answer these questions and inform requirements. Major General Morrison (Commanding General, U.S. Army Cyber Center of Excellence and Fort Gordon) said as much when he stated that "Cyber Quest will concentrate on enabling more rapid technology to aid the soldiers."[11] Similarly, Cyber Blitz is an experimentation campaign supporting the U.S. Army with the timely transition of innovative Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technical capabilities.[12] However, informing warfighters of the results of these events and getting their feedback may still require further progress. These events fall short of emulating an actual tactical environment and are not funded or resourced except for a fraction of the devices and services found in actual units. These issues represent a clear gap in rapidly validating new tools and getting them into the hands of warfighters. Resourcing also hinders operator led design.

Advantages that the U.S. Army have in cyberspace and EW operations are that Soldiers are resourceful, and they are capable of innovating in the field, yet, some EWC2 participants stated that higher headquarters might be hesitant to allow such innovations without proper validation and certification. What is interesting about these questions is that many EWC2 participants believe that there is a need for some level of cyberspace and EW operations capability to be organic to warfighters at DIV-BCT. This lack of communication or shared vision likely serves as a friction point across the Army's leadership. Perhaps Army leadership should reevaluate what capabilities, if any, should be passed down to lower echelons and then educate leadership and staff as to why other capabilities are best suited for execution at the Army Service Component Command (ASCC) level (i.e., ARCYBER).

Some working group (WG) participants also stated they believe there is friction with authority as it applies to training and operations. The perception, whether true or not, is that very few leaders, lawyers, and legislators are competent in cyber law, policy and operations. This gap potentially prevents requests from being generated and staffed at BCT-DIV. Because of this observation, workshop attendees asked what mechanisms exist or could be created to tutor senior leaders (COL and above) who are currently in command and staff positions to close their education gaps in cyberspace operations and policy. A similar question included legislators: what mechanisms exist or could be created to tutor legislators to make more informed policy decisions regarding Cyber/EW.

Workshop participants also questioned how many BCT or Special Forces Group (SFG) Judge Advocate General (JAG) officers possess the competency to inform a legal brief describing whether an internally generated cyber training or operations concept is legal? Perhaps a more important question regarding the use of JAG officers is at what point in training/deployment preparations should a JAG officer be integrated into the military decision-making process (MDMP) for CEMA planning and COA development? If achieved, would integrating the JAG officer into the Cyber/EW planning process could also help close individual education gaps of commanders and staff about cyberlaw?

VI. EMPLOYMENT OF AI/ML IN EW/CYBER OPERATIONS

To effectively employ EW and cyberspace operations at “machine speed” in future, multi-domain operations, workshop participants discussed the incorporation of artificial intelligence/machine learning (AI/ML) in future systems. This could help overcome training lapses and hasten the response time of U.S. Forces to respond to EW- and cyberspace-based attacks. The ability for EW and cyberspace systems to autonomously detect, characterize, and respond to signals of interest will be increasingly important to protect against electronic attack, to deny signals, or to manipulate signals for exploitation. During TechNet 2018, Colonel Steven Rehn, TRADOC Capability Manager (TCM) for Cyber at Fort Gordon, GA, offered several areas where AI can aid EW and cyberspace capabilities. For instance, he stated the application of AI could help reduce the time needed for EW and cyberspace systems to reconfigure and change techniques (or tools) to enable and protect friendly forces’ access to EMS and information systems (IS) while denying adversaries access to the same.

During the workshop, participants discussed what AI/ML is, its applicability to cyberspace and EW operations, and some of the challenges that must be addressed. In general, AI is a set of algorithmic approaches for improving the functionality and performance of a computational system. It reduces the workload of system operators, so they can focus on higher-level, cognitive tasks.[13] In effect, the underlying software is more intelligent and, reduces the number of low-level tasks that one must perform. For example, a voice recognition system reduces the amount of keyboard input. We can think of AI in terms of three overarching goals.

First, some AI emulates *intelligent behavior*. These systems attempt to act as a human would, regardless of whether the underlying sensing or computations are human-like. Driverless cars are a good example: the goal is to have these cars drive like a human would, or perhaps even better. Many times, little regard is given to the corresponding human analogy of the underlying sensors (e.g., LIDAR vs. eyes) and computations (e.g., search algorithm vs. visual-spatial reasoning). A second goal is the emulation of *intelligent thinking*. For example, Amazon's Alexa and Google's Home receive human voice as an input, perceive the verbal question through an ML model, encode it into an internal knowledge representation, decide on an answer through knowledge search, and then encode and deliver an audio response. Finally, some AI goals are to surpass *human performance*. State of the art image recognition systems are now equaling, or in some cases, superseding human performance. A recent example is how DeepMind researchers recently defeated the Alpha Go world champion by training a deep reinforcement learning model to defeat itself and ultimately others through self-play.[14]

Today, we see the beginning of ML as a signal modulation (e.g., APSK, PSK, QAM, etc.) classifier. Past approaches relied heavily on hand-engineered feature extractors for specific signal properties along with rigid decision boundaries. These knowledge-crafted detectors created oversimplifying assumptions, making it difficult to adapt to new signals or emitters. Recently, some have trained convolutional deep neural networks (DNNs) with raw in-phase-quadrature (I/Q) data to classify modulation schemes with results well over 80% for high signal-to-noise ratio (SNR)—above 10dB, delivering some promising results.[15] Still, these approaches for modulation classification are not without challenges. The current state-of-the-art is only useful at high SNR levels and with higher-order modulations being more difficult to classify at lower SNR. Moreover, the nature of DNN makes explainability and errors difficult to interpret, which affects trust. For instance, there is no set of features a DNN can offer an operator to explain why the classifier reached its decision.

Participants identified three key challenges to employing AI/ML in EW/Cyber operational systems. The first is identifying and developing an infrastructure to support the research and development of these systems. This infrastructure includes the collection and storage of data for ML algorithms; the DevOps environment to support rapid prototyping and testing with this data and other developed models; and the experimentation ecosystem (simulated, emulated, and live) to support the development of operational concepts and to provide feedback to engineers. To that end, the DoD's Joint AI Center (JAIC) is working towards such a foundational infrastructure, albeit perhaps without a focused eye towards some of the implications discussed here for EW and cyberspace operations development.

The second challenge, as with any AI/ML program, is that the data acquisition, ingestion, and curation (a.k.a. the data pipeline) becomes an increasingly important component in building reliable systems. This makes raising community awareness for collecting signal data during operations, exercises, and other activities having signals of interest paramount.

Preferably, data is being labeled as it is collected. Often, it is not labeled, so the generation of synthetic data, where labeling can be easily controlled, becomes a default second strategy. Research must determine how to generate such cognitively plausible data streams with realistic, underlying physical signal characteristics. It must also simultaneously develop techniques to transfer learned AI/ML models, trained by synthetic data or real over-the-air (OTA) signals. Research is also needed to evaluate techniques to speed up learning, such as re-training the last few layers of a deep neural network or compensating for lack of data with generative adversarial networks.

Data and algorithm issues with sensors, storage, and compute locations must also be addressed given the disparity between the low bandwidth, high latency tactical edge and the cloud environment where most development and ML training occurs. For context, learning in AI may occur offline or online. Offline learning involves training the system, typically on millions of samples, outside of its operating environment before it is deployed to the production system (e.g., training a surveillance system with many images). Alternatively, online learning is when the AI system uses continuous data from its operating environment to refine its decision-making parameters. Participants recognized that online learning is important as military operations often occur in austere environments where connectivity to the "cloud" is intermittent at best. The ability for the system to learn online from both environmental cues and operator provided hints, requires other types of AI learning, such as reinforcement and episodic (i.e., analogy-based learning). This type of AI learning's applicability to signal detection, characterization, and response is not as well studied as offline deep learning approaches.

The above two challenges involve some research but are primarily engineering challenges. The last challenge identified was more fundamental, as it involves the issue of trust between the human operator and the AI system. This challenge is brought up in many other military contexts when talking about the relationship between the human operator and their military tools, such as one's rifle or tank, so we will not belabor the point here but rather point out some of the unique challenges with AI/ML systems. As mentioned above, the lack of transparency, or explainability, of non-symbolic ML approaches makes it difficult for human operators to understand how the underlying system inferred its classification. Without this understanding, it makes it more difficult for operators, especially experienced operators, to trust the system without a lot of training. Augmenting these non-symbolic approaches with references to symbolic, interpretable representations which make grounded explanations possible, is one approach to mitigate this shortcoming.

Adversarial ML[6] is another issue that decreases trust in the AI/ML system if not properly addressed. In effect, adversarial ML is the ability to "spoof" an ML algorithm to classify a sample the way an adversary desires versus the way the model was trained. Through slight, unrecognizable perturbations in the input signal, adversarial ML takes advantage of the model's classification boundaries, or manifolds, and the model misclassifies the sample.

Dr. Jacob H. Cox Jr., received his BSEE from Clemson University, SC in 2002, his MSECE from Duke University, NC in 2010, and his Ph.D. in ECE from Georgia Institute of Technology in 2017. As an Army officer with 21 years of active service (1996-2018), Jacob has served as a Cyber officer, a telecommunications engineer, and a signal officer. His assignments include company command at Fort Gordon, Georgia (2006-2008); Assistant Professor at the United States Military Academy (2010-2013), and Chief of Enterprise Operations at the South West Asia Cyber Center in Kuwait (2013-2014). Following his Army career, Jacob worked as a research scientist adapting artificial intelligence solutions to cyberspace operations, electronic warfare operations, and decision support. Jacob currently works as the lead data scientist at TCM Cyber, Fort Gordon, GA.

Colonel Dan Bennett, Ph.D., joined the Army Cyber Institute in 2015. He is the Director of Research since serving a one-year operational experience (2016-2017) as the Technical Director Advisor to the Commander of the Cyber National Mission Force at Ft. Meade, MD where he led cyberspace operations infrastructure initiatives in particular. Col. Bennett came to the ACI from the Department of Electrical Engineering and Computer Science (EECS) at the U.S. Military Academy where he still teaches as an Associate Professor. Col. Bennett's previous operational experiences include the lead network engineer for the 101st Airborne Division (Air Assault) which included 15 months as the Director of the Joint Network Operations and Security Center for Combined Joint Task Force – 101 in Afghanistan. Col. Bennett has a Ph.D. in Electrical Engineering specializing in Communications and Digital Signal Processing.

Colonel (Ret.) Scott Lathrop, Ph.D., CISSP, is a visionary technology leader in AI, cybersecurity, and autonomous, unmanned systems. Dr. Lathrop retired from the United States Army, culminating his military career as the Director of Advanced Capability and Technology at the United States Cyber Command (USCYBERCOM) where he led the command's research and development efforts while serving as the chief scientist and technology officer for the Commander, United States Cyber Command/Director, National Security Agency. Prior to USCYBERCOM, Dr. Lathrop served as an Associate Professor in the Department of Electrical Engineering and Computer Science at the United States Military Academy (USMA) helping design and lead USMA's initial cybersecurity and robotics programs. He is a distinguished graduate from West Point and holds a Ph.D. in Computer Science and Engineering from the University of Michigan and received the Army's Draper Leadership Award as an Armored/Cavalry commander, led the development of some of the Army's first cloud-based command and control analytic applications, and has been recognized for teaching and research excellence.

This effect, coupled with the lack of explainability in how these inferences are made can quickly erode trust if the operator suspects malplay. To help build trust, participants expressed the need to bound the behavior of the AI/ML system through interaction and the ability to express what the system's high-level goal(s) and tasks are for the current operational mission—in much the same manner that one would direct a small unit or individual soldier.

Finally, as to the application of AI to enhance EW and cyberspace capabilities, participants asked that leaders and researchers consider which systems and platforms in current use could benefit from autonomy. Participants noted that humans might place too high an expectation on autonomous systems to perform flawlessly and expect too much too soon. 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 cannot account for all the system's data in real-time when it makes an error, who gets blamed for the error when it occurs? These are challenges and ethical considerations for future discovery.

VII. LEVERAGING EW AND CYBER FOR IO

US adversaries have already successfully leveraged the cyberspace domain to conduct information operation (IO) campaigns. Due to the restrictions on U.S. military operations from Title 10 (the role of the Armed Forces), Title 32 (National Guard) and Title 50 (National Defense) mandates, the flexibility and options used by our adversaries to gain advantage are not readily at the disposal of U.S. Forces. Given the nature of a cyberspace war that would place U.S. Forces in near constant competition with our adversaries, we must ask what that line of delineation between competition and conflict regarding the execution of Title 10, 50, and 32 operations is? Workshop participants observed that the line between competition and conflict is not easily defined. Given that traditional military operations are addressed and executed through a phased approach, the planning and execution phases of EW/Cyber operations are difficult to pinpoint.

The difficulty in identifying the phases of a war in cyberspace is further compounded when we attempt to apply traditional operational doctrine to the situation, specifically, the execution of IO in accordance with Joint Publication (JP 3-13). It characterizes IO as the integrated employment, during military operations, of Information Related Capabilities (IRC's) in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. The phrase, "during military operations," could be difficult to identify. JP 3-13 goes on to say that many military capabilities contribute to IO and should be taken into consideration during the planning process, including strategic communications, public affairs, civil-military operations, information assurance, space operations, military deception, joint electromagnetic spectrum operations, and cyberspace operations. In this description, cyberspace operations and information assurance are listed as distinct entities from electromagnetic spectrum operations.

Mr. Chris Walls is a retired Cyber Warfare Officer and is currently a Lead Cyber Security Engineer with the MITRE Corporation. He was commissioned as an Infantry Officer and served in both mechanized and airborne units with numerous combat deployments. In 2010, Chris began his cyber career at US Cyber Command and subsequently served operational and institutional assignments at Army Cyber Command, Army Cyber Center of Excellence, and in HQDA G/3/5/7 Cyber Directorate (DAMO-CY). Among his many distinguished accomplishments, he most recently led the development of Army Field Manual 3-12 Cyberspace and Electronic Warfare Operations, assisted in the design of the Army's new Cyberspace and Electronic Warfare units, and is an acknowledged expert on full spectrum cyberspace operations within the Department of Defense. The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author..

CW4 (RET) Jason LaClair, joined the Army in September of 1995 and attended Basic training at Fort Jackson, SC. He then reported to Advanced Individual Training in Pensacola, FL. Jason has been a career military intelligence (MI) Soldier with assignments including the National Security Agency, the Space and Missile Defense Command, the 4th Infantry Division, the National Reconnaissance Office and Army Cyber Command. He has been deployed to Iraq and Afghanistan and served temporary duty in Korea, India and New Zealand. Jason attended the Intermediate Signals Analysis Course, warrant officer Basic Course, warrant officer Advanced Course, Air Assault and Airborne School. Jason's awards include the Legion of Merit, the Bronze Star and the Commander's Award for Civilian Service. Jason has a Bachelor of Science from the University of Alabama and is pursuing a Master of Public Administration from Penn State University. Jason currently works as a defense contractor and resides in Augusta, GA.

Lieutenant Colonel Clint Tracy was commissioned from Texas A&M University as an Armor Officer and served in leadership positions in Armor Battalions from 1998 to 2006. From 2006 to 2010 he was assigned to Operations Group, National Training Center, Fort Irwin, California and the Canadian Maneuver Training Center where he served in observer controller positions providing feedback to units preparing for Operations Iraqi Freedom and Enduring Freedom. In 2011 he attended CGSC and simultaneously earned a M.S. in IT Management. From 2012 to 2016 he served as the G35 1st Infantry Division, a Cavalry Squadron XO, Brigade S3, Brigade Deputy Commander, Provisional Brigade Commander, and the Theater Army Branch Chief for TCM EAB. In 2017 he transitioned to Electronic Warfare and is currently the CEMA Chief for the 1st Cavalry Division where he integrates Cyber and Electronic Warfare into tactical operations. LTC Tracy has combat experience in Iraq and Afghanistan.

The mission of ARCYBER is to "conduct full-spectrum cyberspace operations, electronic warfare and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries." One could argue the mission of ARCYBER is, in part, to conduct IO. Already, ARCYBER is in the process of categorizing many of the separate operations above (EW, IO, and cyberspace operations) under the umbrella of "information warfare." The term "Information Warfare" is not yet defined in our doctrine; however, the initiative stems from NDAA Sections: 1637 - Integration of Strategic Information Operations and Cyber-Enabled Information Operations; and 1641 - Plan to Increase Cyber and Information Operations, Deterrence, and Defense to Develop a "Strategic Framework for the conduct of DoD IO." However, according to BG Angle, the role of the ARCYBER Commander may be short-lived, becoming a subset of IO, while the name of ARCYBER could soon become something close to Information Warfare Operations Command.

Recognizing this, a closer look at how and when IO planning occurs is in order. JP 3-13 is clear, "IO planning begins at the earliest stages of [the] Joint Operations Planning Process (JOPP) and must be an integral part of, not an addition to, the overall planning efforts. IRCs can be used in all phases of a campaign or operation, but their effective employment during the shape and deter phases can have a significant impact on remaining phases." When do these "shape and deter" phases begin and end? The conduct of IO must have an appreciation for the inter-related capabilities of cyberspace operations, (both defensive and offensive), EW, and signals intelligence—most importantly for assessing the effectiveness of IO. Due to the length of time needed to identify, develop, and deploy cyberspace operations tools, waiting until phase 0 to begin the process (especially the process of collection management from an intelligence perspective) will likely not deliver the desired effects when needed. Perhaps no kinetic operation is warranted if a shape and deter IO campaign is effective in quelling any conflict before it begins.

The Army, specifically the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO-IEWS), views Information Warfare as the complementary components of intelligence, cyberspace operations, EW, and signal. Each of these elements is a potential tool for conducting Information Warfare. With that, the acquisitions process is being adjusted to meet the needs of warfighters with more agile acquisition processes and best-of-breed application of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) capabilities. One expects the doctrine to evolve with the capabilities. Cyberspace operations and capabilities will also impact the Commanders' decisions in the arena of "intelligence gain/loss" like never before. New questions will seek to determine whether the delivery of content in an IO campaign will rival the Commander's ability to disable an adversaries' communications network? These are challenges that U.S. commanders have not faced on linear battlefields in the past, but emerging technology is bringing enhanced cyberspace and EW operations to the forefront.

CW4 Judy Esquibel is an active duty Cyber Operations Technician. She is currently assigned as an Information Sciences Ph.D. student, at the Naval Postgraduate School, Monterey, CA. Formerly, she served at the Army Cyber Institute (ACI) and as an Instructor within the Electric Engineering and Computer Science Department, U.S. Military Academy, West Point, NY. Her research efforts at the ACI focused on improving critical infrastructure protection, public-private partnerships and cyber exercises. Some of her results and conclusions were codified in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to enhance the nation's critical infrastructure security. Her operational experience includes 20 years of Signals Intelligence and Cyber operational assignments, which include being assigned on a Combat Mission Team, within the Cyber Mission Forces, U.S. Cyber Command.

Cyber is inherently a joint operation. Just as the Navy has re-badged numerous elements within their formations to present a better-defined mission focus, and consolidate talent and resources, so too shall the Army. Challenges facing the Army will be which flags are to be furled and which are to be flown. As the Army decided between intelligence and signal to give birth to a cyber element, similar decisions now must be made about acquisitions, requirements, training, and doctrine supporting elements. Training must be the most pressing item. Is this a maneuver effort, an intelligence function, or a cyberspace operation? A kinetic or non-kinetic fight? Is the Information Officer on staff equipped to take on such a task? Cyber Intelligence is not a recognized category, but the operational information gleaned from cyberspace operations certainly carries intelligence value. How is the relationship between the staff intelligence officer, operations officer, and signal/communications officer meeting the commander's requirements to protect his or her network while potentially exploiting or denying the adversary use of their own? Cyber Electromagnetic Activities cells (see FM 3-38) are operational elements at the Division level, but the IO campaigns from which they feed and obtain information will likely be conducted at the theater level.

The categorization of IO as a kinetic or non-kinetic capability is not a simple task. If, when learning that an adversary has disabled a Bradley via a cyberspace operation (a phase 0 activity) in an information warfare campaign and the crew then abandons that Bradley, the vehicle is effectively destroyed, similar to a kinetic effect. Adversely, if counter-cyberspace operations (defense) are effective in keeping the adversary from disabling the Bradley vehicle, it can deal a blow to the adversary's battle plan, both kinetically and from an information warfare perspective. Then, how useful can efforts before phase 0 of an operation to obtain the information needed to access networks, impact social media users, degrade GPS, or disrupt communications? The simple demonstration or application of these capabilities may negate the need for further escalation. Perhaps these efforts could be the decisive actions during phase I, II, III or beyond in the Operation Plan (OPLAN), but they would not be available if the planning phase was not enacted until phase 0. Part of the challenge will be proving that the desired effects can be met via cyberspace operations where kinetic effects have traditionally persevered. Combatant Commanders trust visuals of smoking craters more than percentages (or probabilities) of success based on mathematical equations. This will require the inclusion of new, modular, and data-driven battle damage assessment (BDA) tools for IO.

In closing, leveraging cyberspace and EW operations to facilitate IO opens a wide spectrum of possibilities to warfighters, potentially winning wars before they are fought. Already, EW is listed as one of the five core capabilities of IO.[17] At a minimum, conducting IO at the earliest possible opportunity will give Commanders an advantage during subsequent phases of the battle. However, the correct characterization and application of IO are required. The manning, training and equipping of those expected to execute IO also deserves appreciation and attention by commanders and given a priority of effort.

VIII. CONCLUSION

As near-peer adversaries continue to develop and employ increasingly advanced technologies in multi-domain battle, the US is challenged to hone its EW and cyberspace operations into carefully integrated capabilities. Naturally, the merger of EW and Cyber comes with challenges, friction points, and gaps that must be overcome for U.S. Forces to thrive in multi-domain battle. The EWC2 workshop identified multiple challenges and opportunities where these issues can be addressed. As such, this work merely offers questions and leaves the real work to other researchers, policymakers, and leaders to answer. Additionally, while the EWC2 workshop's focus began with the convergence of EW and Cyber, it is apparent that even these may only be part of the larger whole. In the future, other components, such as IO, Psychological Operations, Intel, Space, and Signal, may soon join the merger.

Participants also discovered that the Army is already conducting a study to ascertain how all of these groups might fit under the umbrella of Information Warfare Operations. Perhaps a circus tent would be apropos considering how these disparate disciplines must learn to complement one another. Regardless of terminology, the concepts behind Information Warfare Operations must be further refined. To accomplish this feat and dominate future conflicts, the U.S. and its allies must work together to address friction, close gaps, and embrace evolving technologies within EW and cyberspace operations, incorporating other disciplines where it makes sense. With near-peer adversaries investing in EW and cyberspace operations, rapidly building and employing their capabilities, the U.S. must aggressively tackle these challenges or face a future conflict where information superiority is not achieved.

ACKNOWLEDGMENTS

The authors would like to extend our thanks to the organizations and individuals who contributed to the workshop's success. This workshop would not have been possible without the support of the Army Cyber Institute (ACI) at West Point, NY and the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center at Aberdeen Proving Ground (APG), MD. We especially thank our volunteers MAJ Joseph Kosturko; Mr. Giorgio Bertoli, CPT Ian Bolster, CW2 Brandon Chapelo, CW3 Benjamin Holladay, Ms. Caitlyn Byrne, and Dr. Michael Lilienthal for their leadership and assistance with the working groups.

DISCLAIMERS

The views expressed in this paper are those of the authors and not of their organizations; they are not to be construed as an official Department of the Army position unless so designated by other authorized documents. Citation of manufacturers' or trade names does not constitute an official endorsement or approval of the use thereof.

Approved for Public Release; Distribution Unlimited. Public Release Case Number 19-2915

NOTES

1. Field Manual, "FM 3-12 Cyberspace and Electronic Warfare Operations," April 2017.
2. CERDEC has since been rechristened as the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center.
3. Cyber electromagnetic activities (CEMA) are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0).
4. Some refer to these types of non-physical engagements as "non-kinetic", for example see https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474091.
5. S. Cohen, "Integrating Cyber and Electronic Warfare," The Cyber Edge, Signal, March 2018.
6. Joint Chiefs of Staff, "Joint Publication 3-13.1 Electronic Warfare," February 8, 2012.
7. Joint Chiefs of Staff, "Joint Publication 3-12 Cyberspace Operations." June 8, 2018.
8. M. Senft, "Convergence of Cyberspace Operations and Electronic Warfare Effects," *The Cyber Defense Review*, January 4, 2016.
9. P. Frost, C. McClung, C. Walls, "Tactical Consideration for a CDR to Fight and Win in the EMS." *The Cyber Defense Review*, Vol 2 No.1 Spring 2018.
10. "Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)," Combined Arms Center -Capability Development Integration Directorate (CAC-CDID), December 2010.
11. D. Johnson, "Fort Gordon kicks off 2018 Cyber Quest." NextStar Broadcasting, Inc. June 22, 2018.
12. "CYBER BLITZ." Combat Capabilities Development Command C5ISR Center, U.S. Army, [Available] Online https://www.cerdec.army.mil/inside_cerdec/cyberblitz/index.php.
13. S. Trent and S. Lathrop, "A Primer on Artificial Intelligence for Military Leaders," *Small Wars Journal*, August 23, 2018.
14. David Silver, Julian Schrittwieser, Karen Simonyan, Ioannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert, et al., 2017, "Mastering the Game of Go without Human Knowledge," Nature 550 (October), 354.
15. Timothy James O'Shea, Tamoghna Roy, and T. Charles Clancy, "Over-the-air deep learning based radio signal classification." IEEE Journal of Selected Topics in Signal Processing 12.1 (2018), 168-179.
16. Daniel Lowd and Christopher Meek, 2005, "Adversarial Learning," In Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, KDD '05, New York, NY, USA: ACM, 641–647.
17. Joint Chiefs of Staff. "Joint Publication 3-13.1 Electronic Warfare," February 8, 2012.