CEMAlite Virtual Summit
SEPTEMBER 29, 2020
Online Virtual Event

CEMAlite Virtual Summit
Post-Event Report

October 5, 2020

Table of Contents

About the AOC

ASSOCIATION OF OLD CROWS

Advancing Electromagnetic Warfare TOGETHER
crows.org

With over 14,000 members internationally, the Association of Old Crows (AOC) is an organization for individuals who have common interests in Electronic Warfare (EW), Electromagnetic Spectrum Management Operations, Cyber Electromagnetic Activities (CEMA), Information Operations (IO), and other information related capabilities. The AOC provides a means of connecting members and organizations nationally and internationally across government, defense, industry, and academia to promote the exchange of ideas and information, and provides a platform to recognize advances and contributions in these fields.

AOC Issue Brief:
The Evolution of Army CEMA

The Emergence of CEMA

Cyber Electromagnetic Activities (CEMA) is an US Army concept for conducting operations in Cyberspace and the Electromagnetic Spectrum.

CEMA doctrine began to take shape in the 2010 timeframe. The Army was already embracing cyber operations by this time, and its ground forces had spent the previous six years investing in automated low-power communications jammers to combat RCIEDs in Iraq and Afghanistan. As the Army became more committed to the electronic warfare (EW) mission from 2006 onward (it formally established an EW career field in 2010), its leaders wanted to articulate how EW and cyber operations would be conducted together in future operations. CEMA would be developed to provide this synergistic framework.

In February 2014, the Army released its first CEMA doctrine, FM 3-38, which described "the importance of cyberspace and the electromagnetic spectrum (EMS) to Army forces and provides the tactics and procedures commanders and staffs use in planning, integrating, and synchronizing CEMA." In April 2017, it issued FM 3-12 on Cyberspace and Electronic Warfare Operations. This document superseded FM 3-38 and combined "the fundamentals and guiding principles for cyberspace operations, EW, and CEMA in one publication." It also "describes the cyberspace operations, missions, actions, EW, the electromagnetic spectrum (EMS), and the interrelation of these activities among each other and all Army operations. The description includes CEMA as the planning, integrating and synchronizing activity for echelons corps and below." In 2018, the Army began to include signal intelligence (SIGINT) in its CEMA concept, which recognized the contribution that these sensors could provide in building a real-time tactical picture for mission commanders.

The CEMA Approach

It is worth clarifying that CEMA is not a capability in itself. CEMA is a combined arms approach that draws on cyber, EW, spectrum management operations and SIGINT capabilities. CEMA sits at the nexus of these capabilities and exploits their synergy. Within the Army, it enables Division and Brigade commanders to see and understand what is happening in the EM operating environment (information that was not available to commanders in real-time, even recently) so that their forces can effectively maneuver (communicate, navigate, sense, engage targets, etc.) within the EMS.

CEMA is performed by Expeditionary CEMA Teams (ECTs) comprising cyber, EW and spectrum management operators. The ECTs are organized under Army Cyber Command's 915th Cyber Warfare Battalion and they are deployed with Division- and Brigade-level tactical operations centers (TOCs). Prior to the formation of ECTs, Division and Brigade commanders had few EW and cyber resources under their direct control and even fewer experts within the TOC who could task and exploit them. By situating cyber, EW and spectrum management personnel together within the TOC, the ECT can create the synergy the commander needs to understand and maneuver within the EM environment.

Equipping ECTs through CEMA

While the Army has spent the past several years organizing and training its cyber and EW forces under the CEMA concept, it has also focused on equipping its ECTs for real-time operations in the EMS. This includes robust software applications like Electronic Warfare Planning and Management Tool (EW PMT), as well as airborne EW and offensive cyber capabilities like Multi-Function EW - Air (MFEW-Air), and ground-based EW, SIGINT and offensive cyber systems like the Terrestrial Layer System (TLS).

EWPMT

The Electronic Warfare Planning and Management Tool (EWPMT) is a software suite that enables the ECT to plan, coordinate and synchronize electronic support (ES), electronic attack (EA) and spectrum management activities for the mission commander. It is the glue that ties together the ECT's cyber and EW systems, such as MFEW-Air and TLS, across the commander's AOR.

The EWPMT program is being developed by Raytheon Intelligence and Space (Fort Wayne, IN) for PEO Intelligence, Electronic Warfare and Sensors (PEO IEW&S). The Army is fielding EWPMT incrementally via a series of Capability Drops (CDs). CD1 is "foundational" and provides basic EW planning and targeting. CD2 adds spectrum management, as well as modeling and simulation tools. These first two CDs have been developed and fielded. CD3, which is completing development, will enable ECT personnel in the TOC to directly control EW and cyber assets throughout the AOR. CD4, which is also under development, will provide the ability to assess EW effectiveness, add enhanced targeting, as well as remote control and management (RCM). It will also enable EWPMT to interface with the Command Post Computing Environment (CPCE) under development by PEO C3T. These first four CDs comprise EWPMT Increment 1. PEO IEW&S is already planning EWPMT Increment 2, which will focus on transforming the software suite into a more robust Electromagnetic Battle Management (EMBM) capability.

MFEW-AIR

The ECT's primary set of airborne EW capabilities is Multi-Function EW System-Air (MFEW-Air), a family of unmanned aerial systems (UASs) that will perform ES, EA and offensive cyber functions. The first system in the family is MFEW-Air Large, which is currently under development by Lockheed Martin Rotary and Mission Systems (Owego, NY). MFEW-AL is configured in a pod integrated onto the Army's MQ-1C Gray Eagle UAS. ECT personnel can task the system via EWPMT to detect, identify and attack targets. The MFEW Air Large is currently completing Engineering and Manufacturing Development and will begin operational testing in early FY2022. The First Unit Equipped is scheduled for later in FY2022.

In addition to MFEW-Air Large, the Army also envisions developing an MFEW-Air Small system for Group 2-3 UAS and MFEW-Air Rotary Wing for helicopters in the FY2023-2025 timeframe.

TLS

The Terrestrial Layer System (TLS) is a new family of EW/SIGINT/offensive cyber systems housed on tactical vehicles. When the first TLS systems are fielded in FY2022, they will be assigned to the multi-functional platoon and the EW platoon organic to the Military Intelligence (MI) Company (MICO) in the Brigade Combat Team (BCT). TLS will integrate with other ECT elements via EWPMT.

PEO IEW&S is developing TLS in two versions. The standard version of TLS is currently in prototype development, with Lockheed Martin Rotary and Mission Systems (Owego, NY) competing against Boeing's Digital Receiver Technology, Inc. (DRT) (Germantown, MD) for the EMD contract to be awarded in FY2021. This standard TLS will be housed on a Stryker armored vehicle and will support BCT commanders.

Recently, PEO IEW&S announced plans to begin developing a second, larger version known as TLS - Echelons Above Brigade (TLS-EAB) to support Division commanders. Housed on a heavy trailer and a lighter support vehicle, TLS-EAB will be configured in two variants. Subsystem 1 would feature a tethered drone or aerostat to provide long range collection, ES and "effects" against ground and airborne signals of interest. It would be operated by four EW personnel and three SIGINT experts. Subsystem 2, manned by four EW operators, would receive cues from air defense sensors over a network, as well as its own ES sytesms, and perform high-power defensive electronic attack to protect Division assets from threats such as drones, rockets and precision artillery. Program officials are planning to field TLS-EAB beginning in late 2023.

PACING THE THREAT

One lesson the Army learned from the battle against RCIEDS in Iraq and Afghanistan was the difficulty it experienced matching the rapid pace of commercial technology, such as the cell phones, garage door openers and other household electronics used to trigger IEDs. This pacing challenge continues to be problematic as the US confronts near-peer competitors who are exploiting rapidly evolving commercial technologies in their communications systems, sensors, and PNT systems. To match this trend, the Army needs to buy electronics at a faster pace than traditional acquisition programs allow. For this reason, it is making extensive use of technology consortiums and Other Transaction Authority contracting vehicles that offer much shorter development timelines. At the same time, PEO IEW&S is championing the use of C5ISR/Electronic Warfare Modular Open Suite of Standards (CMOSS) to enable rapid prototyping and upgrades in programs such as MFEW and TLS.

GROWING CEMA

The Army first articulated its CEMA concept to enable ground forces –Division and Brigade commanders – to sense and maneuver in the EM Environment. As a result, the Army's initial CEMA architecture is taking shape with EWPMT, MFEW-Air and TLS. However, it's important to understand that this is just a beginning. Ultimately, the Army wants to develop new airborne capabilities that could significantly extend the range and grow the target set of the CEMA architecture. One such program is currently in the early stages of planning and development. The Multi-Domain Sensing System (MDSS) will be integrated onto an airborne platform operating at medium and high altitudes at stand-off ranges. It will feature Electronic Intelligence (ELINT), Communications Intelligence (COMINT), Synthetic Aperture Radar (SAR), Moving Target Indicator (MTI), Cyber/EW, Air-Launched Effects (ALE) and aircraft survivability sensors. The initial MDSS focus area is to develop ELINT and COMINT sensors under an effort named High Accuracy Detection and Exploitation System (HADES). ALE is another early focus area of the program. ALE will utilize small, attritionable unmanned aerial systems to detect, identify, locate, report (DILR) and deliver lethal and non-lethal effects against threats in support of Long-Range Precision Fires.

CEMA and MDO

As the Army embraces Multi-Domain Operations (MDO), its units will depend more than ever on access to, use of, and tactical control over the Electromagnetic Environment. CEMA, as described above, provides the operational concept that will make MDO viable.

CEMAlite Virtual Summit

Presentation Synopsis

The AOC's CEMAlite Virtual Summit was a one-day virtual event that provided attendees an update on emerging EW requirements, policies, Science and Technology (S&T) initiatives, programs to demonstrate how the US Army is evolving its Cyber Electromagnetic Activities (CEMA) architecture to counter Near Peer Competition in the Electromagnetic and Information Environments. The Summit offered five (5) sessions covering Emerging Technologies and Trends, Innovation and Critical Capabilities, the EMS Enterprise, an Operational Perspective, and in conclusion, a session on Acquisition and Program.

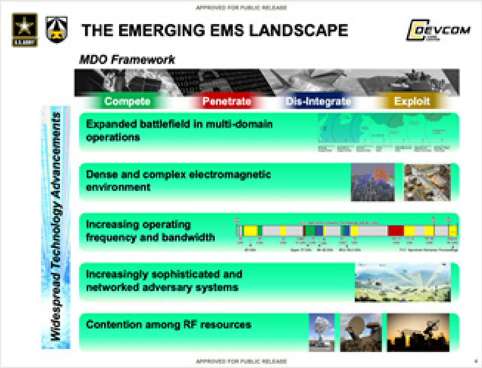
CEMAlite opened with a welcome by **Brigadier General Michael Sloan, Program Executive Officer, Intelligence Electronic Warfare & Sensors (IEW&S)**. To best address the Army's ongoing modernization efforts to ready its force for Multi-Domain Operations (MDO) in 2028, BG Sloan highlighted the need for collaboration and transparency across stakeholders in military, government, and industry. The National Security Strategy and the National Defense Strategy both call for US dominance in the cyber domain and information environment. CEMA is the Army's concept to shape the battlefield and leverage capabilities to seize, retain, and exploit an advantage over adversaries in both cyberspace and the electromagnetic spectrum.

The keynote address was provided by **Lieutenant General Stephen Fogarty, Commanding General, US Army Cyber Command.** LTG Fogarty provided a unifying vison and context for CEMA that focused on its evolution to pursue what he called, "Decision Dominance" in MDO to achieve information overmatch of the adversary and align resources to expand the capacity of Army Cyber, EW, and IO elements. He highlighted that the Electromagnetic Environment (EME) is complex – a challenging mixture of contested and congested manuever space. Adversaries and peer competitors understand our reliance on the EMS and are skillfully using their capabilities – often in the absence of state-of-the-art technology – to erode or prevent our advantage in the EMS. Therefore, it is critical for the Army to consistently evolve and drive EW/Cyber/IO elements and capabilities down to the Brigade Combat Team (BCT) Commander. CEMA, therefore, can be viewed as an intermediate step to, ultimately, an Information Warfare (IW) advantage for the Army.

Following the keynote session, CEMAlite proceeded with *Session 1, Emerging Technologies & Trends*, with **Mr. Giorgio Bertoli, Director (A), C5ISR Center, Intelligence and Information Directorate (I2WD)** as moderator. Mr. Bertoli welcomed **Dr. Alexander Kott, Chief Scientist, ST, CCDC Army Research Laboratory** to discuss Cyber Resilience, which is the ability of systems to resist, absorb, and recover from or adapt to an adverse cyber occurrence during an operation. Dr. Kott noted that Cyber Resiliency is NOT synonymous with Cyber Security – they are not interchangeable terms. Rather, Cyber Resiliency comes into play AFTER Cyber Security fails. Due to the complex characteristics of the Information Environment in modern military operations, the probability of system compromise from a Cyber incident or attack is relatively high. Conventional responses are inadequate. Improvement of cyber resiliency requires autonomous solutions that provide high throughput testing and rigorous and repeatable measurements of effects.

Dr. Paul Zablocky, Strategic Technology Office (STO) Program Manager at DARPA, discussed new, highly distributed technologies in communicating and sensing that both open doors and pose real challenges to the EW community. Such programs include the commercial Starlink initiative and DARPA's BlackJack that leverage thousands of satellites and satellite constellations create an incredibly robust Internet and communication capability. These efforts can improve sensing and data collection, but they can also make "Decision Dominance," as LTG Fogarty said, that much harder to achieve. Dr. Zablocky also discussed DARPA's Resilient Networked Mosaic Communications (RN DMC) that seeks to leverage communication between groups of randomly distributed nodes via low-cost, expendable transceiver elements randomly located near tactical radios to form an antenna array that focuses energy to improve signal-to-noise ratio and suppress interference. Distributed communications and sensing technologies pose challenges to EW operations. These technologies make it difficult to leverage gain from directional antennas to improve jammer-to-signal ratio. Furthermore, they are extremely flexible, highly complex, and massively distributed, making it difficult to pinpoint failures.

Dr. Jeff Boksiner, Senior Research Scientist (ST) for EW at the Army's C5ISR Center closed out the panel to discuss EW S&T for MDO. He focused on the emerging EMS landscape, including the ever-expanding battlefield in MDO, a complex EME with sophisticated and networked adversary systems, and an increasing contention among RF resources. According to Dr. Boksiner, EW S&T for MDO covers a wide array of capabilities and concepts, but importantly, mid-term and the future concepts, include cooperative and autonomous solutions, such as Cognitive and Distributed EW, photonic signal processing, RF resource optimization, simultaneous transmit and receive, and low-noise sensitive receivers.



APPROVED FOR PUBLIC RELEASE

THE EMERGING EMS LANDSCAPE

MDO Framework

Compete | Penetrate | Dis-Integrate | Exploit

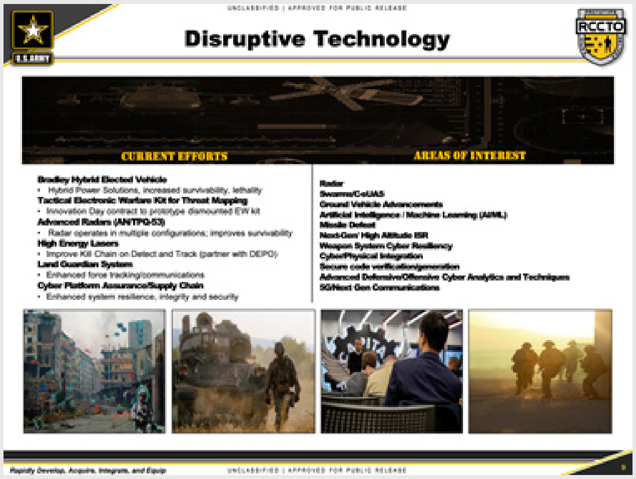
Widespread Technology Advancements

- Expanded battlefield in multi-domain operations
- Dense and complex electromagnetic environment
- Increasing operating frequency and bandwidth
- Increasingly sophisticated and networked adversary systems
- Contention among RF resources

APPROVED FOR PUBLIC RELEASE

Session 2 covered *Innovation & Critical Capabilities* with **Mr. Mike Ryan from the AOC Board of Directors** as moderator. Mr. Ryan welcomed **Major General Peter Gallagher, Director, Army Network Cross-Functional Team (CFT)**. He emphasized the need for unified command and control (C2) and pointed to how the Army's modernization efforts are enabling the Army to deliver critical network capabilities to the Joint force for MDO warfighting. MG Gallagher also shared feedback from Project Convergence 2020, an annual large-scale demonstration and exercise to accelerate decision making and solve technical integration challenges on the battlefield.

Mr. Stan Darbro, Deputy Director of the Army Rapid Capabilities and Critical Technologies Office (RCCTO), followed to discuss Army capabilities and innovations via RCCTO, whose mission it is to rapidly and efficiently develop, prototype, and field critical enabling technologies and capabilities that address near-term and mid-term threats. The RCCTO executes this mission consistent with the Army's modernization priorities that maximize the Soldier's capabilities to deploy, fight, and win on future battlefields. A key innovation focus area is the pursuit of Disruptive Technology. RCCTO current efforts include Tactical EW kit for Threat Mapping, Advanced Radars, and High Energy Lasers (HEL). Additional areas of innovation interest include multi-function radars, swarming C-sUAS, AI/ML and NextGen High-Altitude ISR.


UNCLASSIFIED | APPROVED FOR PUBLIC RELEASE

Disruptive Technology

CURRENT EFFORTS

Bradley Hybrid Elected Vehicle
- Hybrid Power Solutions, increased survivability, lethality

Tactical Electronic Warfare Kit for Threat Mapping
- Innovation Day contract to prototype dismounted EW kit

Advanced Radars (AN/TPQ-53)
- Radar operates in multiple configurations; improves survivability

High Energy Lasers
- Improve Kill Chain on Detect and Track (partner with DEPO)

Land Guardian System
- Enhanced force tracking/communications

Cyber Platform Assurance/Supply Chain
- Enhanced system resilience, integrity and security

AREAS OF INTEREST

Radar
Swarms/C-sUAS
Ground Vehicle Advancements
Artificial Intelligence / Machine Learning (AI/ML)
Missile Defeat
Next-Gen/ High Altitude ISR
Weapon System Cyber Resiliency
Cyber/Physical Integration
Secure code verification/generation
Advanced Defensive/Offensive Cyber Analytics and Techniques
5G/Next Gen Communications

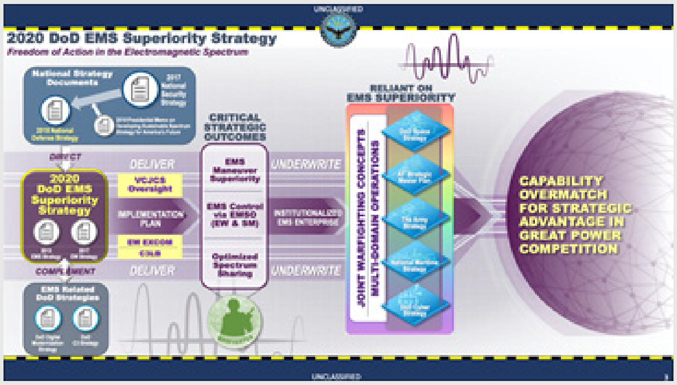
Rapidly Develop, Acquire, Integrate, and Equip

UNCLASSIFIED | APPROVED FOR PUBLIC RELEASE

Next, the CEMAlite Virtual Summit Title Partner, Perspecta, hosted a Lunch and Learn session to share "Real-Time Spectrum Awareness for the Battlefield." Ms. Jennifer Napper, (ret.) Major General, and Vice President of Perspecta's Army Segment, and Mr. Andrew Portune, a Senior Research Scientist, introduced Perspecta's Secure Sense program. According to Ms. Napper, Secure Sense delivers near real-time intelligence on spectrum usage at specific places, times, and frequencies. It also provides adaptive management of a sensing network, signal processing techniques, and an ability to analyze current and historical data, allowing for the discovery of unexpected emitters in highly-cluttered environments. For more information on the program, please visit www.perspecta.com.

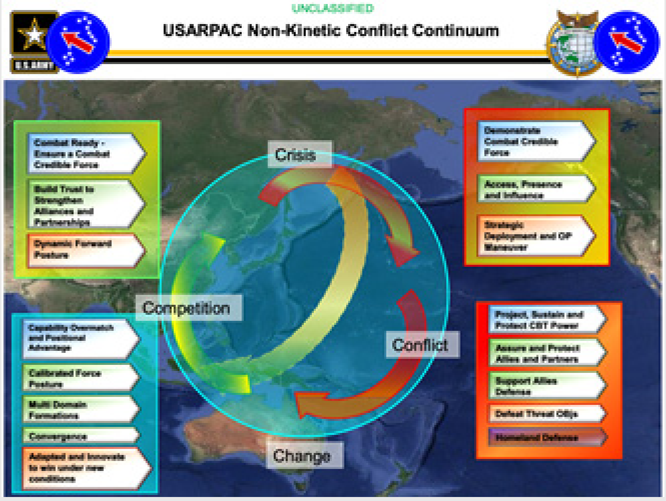
perspecta™

The afternoon of the Summit began with Session 3, which focused on the EMS Enterprise, chaired by **Mr. Jesse "Judge" Bourque, Special Advisor to the Secretary of Defense Electromagnetic Spectrum Operations Cross Functional Team (EMSO CFT)**. He welcomed **Brigadier General Darrin Leleux, USAF, Deputy Director of the EMSO CFT** who provided an update on the pivotal and forthcoming 2020 EMS Superiority Strategy that will focus on three critical outcomes: (1) EMS Maneuver Superiority; (2) EMS Control via EMSO, which includes both traditional EW and Spectrum Management and is aligned with recent Joint Publication 3-85; and (3) Optimized Spectrum Sharing. Gen. Leleux reiterated that all joint warfighting concepts in MDO are reliant on EMS superiority for strategic advantage against peer competitors. He was followed by **Mr. Adam Nucci, DISL, Deputy Chief of Staff, G-3/5/7 Deputy Director of Strategic Operations**. Mr. Nucci shared how the Army is transforming readiness at the tactical, operational and strategic levels and how this requires a layered convergence of cyber, space ISR, EW, and long-range precision fires to achieve a decisive advantage against adversaries. A fundamental challenge to achieving EMS Superiority is that the EMS must be understood and operationalized before military forces are in theater. We must start the understanding of


UNCLASSIFIED
2020 DoD EMS Superiority Strategy
Freedom of Action in the Electromagnetic Spectrum
National Strategy Documents
2017 National Security Strategy
2018 National Defense Strategy
DIRECT
2020 DoD EMS Superiority Strategy
COMPLEMENT
EMS Related DoD Strategies
DELIVER
VCJCS Oversight
IMPLEMENTATION PLAN
EW EXCOM CSLR
DELIVER
CRITICAL STRATEGIC OUTCOMES
EMS Maneuver Superiority
EMS Control via EMSO (EW & SM)
Optimized Spectrum Sharing
UNDERWRITE
INSTITUTIONALIZED EMS ENTERPRISE
UNDERWRITE
RELIANT ON EMS SUPERIORITY
JOINT WARFIGHTING CONCEPTS
MULTI-DOMAIN OPERATIONS
DoD Space Strategy
AF Strategic Master Plan
The Army Strategy
National Maritime Strategy
DoD Cyber Strategy
CAPABILITY OVERMATCH FOR STRATEGIC ADVANTAGE IN GREAT POWER COMPETITION
UNCLASSIFIED

how to build windows of opportunity against the adversary in the competition, crisis, and conflict phases. To do this, the Army is dedicated to delivering three Multi-Domain Operations tenets: (1) calibrated force posture; (2) multi-domain formations; and (3) joint freedom of action.

Session 4 provided an operational perspective featuring a panel moderated by **Lieutenant Colonel Mike Brock, Asst ACM-EW/US Army Cyber Center of Excellence, Army Capabilities Manager - Electronic Warfare**. LTC Brock welcomed **Colonel Clint Tracy, III Corps CEMA Chief, Deputy G3, G35**, and **Colonel LJ Jordan, US Army Pacific Command (USARPAC)**. COL Tracy focused on the application of CEMA in large scale combat operations (LSCO). The contested EMS in LSCO presents a challenge to identify, track and prosecute high value targets. Forces must parse through the prevalence of low-cost, highly distributed, and oftentimes commercially available adversary radars, jammers, communications, emulators, and civilian emitters. COL Jordan looked closely at the Asia-Pacific strategic environment that features "hyper-competition" as China pursues regional hegemony, North Korea seeks regime survival, and violent extremist organizations are expanding through South Asia. The US military has tremendous opportunities for regional engagement and the strategic environment demands multi-domain operations in collaboration with allied forces. USARPAC is working to bring MDO from concept to application. One way the Army is pursuing this opportunity is through cross-domain fires in joint combined maneuver to seize, retain, and exploit the initiative from a CEMA perspective to ensure US and allied forces can achieve freedom of maneuver in the EMS.



UNCLASSIFIED

USARPAC Non-Kinetic Conflict Continuum

Combat Ready - Ensure a Combat Credible Force

Build Trust to Strengthen Alliances and Partnerships

Dynamic Forward Posture

Crisis

Competition

Conflict

Change

Capability Overmatch and Positional Advantage

Calibrated Force Posture

Multi Domain Formations

Convergence

Adapted and Innovate to win under new conditions

Demonstrate Combat Credible Force

Access, Presence and Influence

Strategic Deployment and OP Maneuver

Project, Sustain and Protect CBT Power

Assure and Protect Allies and Partners

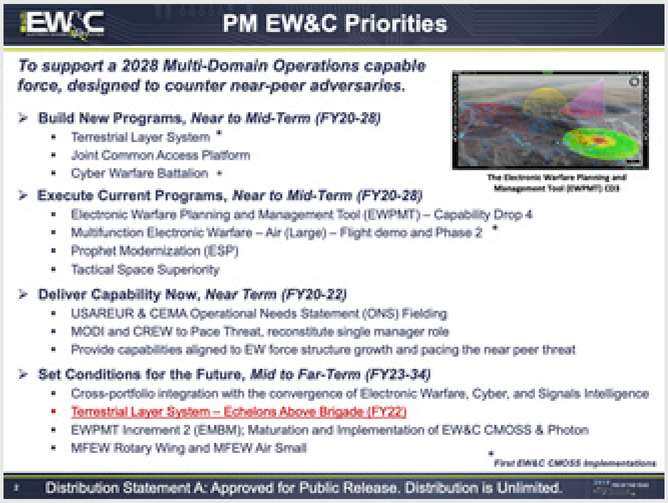
Support Allies Defense

Defeat Threat OBJs

Homeland Defense

The fifth and final session was on CEMA Acquisition and Programs and featured two panels moderated by **Mr. Willie Utroska, Deputy Project Manager, Electronic Warfare & Cyber (EW&C)**. The first panel focused on the Army's Terrestrial Layer System – Echelons Above Brigade (TLS-EAB). Presenters included **Colonel Kevin Finch, Project Manager, EW & Cyber (PM EW&C), Colonel Daniel Holland, Army Capability Manager for Electronic Warfare,** and **Colonel Jennifer McAfee, Army Capability Manager for Terrestrial & Identity.** TSL-EAB is an ISR Task Force priority and intended to provide commanders at echelons above brigade the ability to sense, provide improved precision geolocation, conduct non-kinetic fires, and support kinetic targeting for broad coverage of targets. TLS-EAB can also provide defensive electronic attack (EA), including denying adversary ISR, and disrupting RF guided munitions. Specifically, it is a networked and integrated SIGINT, EW, & Cyberspace Operations System enabling deep-sensing and effects capabilities at the Theater Army level, Corps, & Division to support MDO Aimpoint Force 2035 during competition and armed conflict. TLS-EAB leverages the EMS and resilient, robust mesh networks to detect, identify, locate, deny, disrupt, degrade, destroy, manipulate, and influence the threat.

COL Finch followed by discussing more broadly the PM EW&C portfolio. TLS-EAB, along with the Joint Common Access Program (JCAP) and the Cyber Warfare Battalion (CWB), are the top 2028 MDO new programs. TLS-EAB and CWB will also be among the first CMOSS suite of open standards implementations. Additionally, COL Finch also highlighted the necessity for setting conditions in the Army for the future fight, looking at the FY 2023-2024 timeframe. Those conditions include four pillars, including Cross-portfolio integration with the convergence of EW, Cyber, and SIGINT; the TLS-EAB scheduled to arrive by FY 2024; the EW Planning and Management Tool (EW PMT) Increment 2, which delivers EM Battle Management (EMBM) capability; and Multi-Function EW (MFEW) Rotary Wing and MFEW Air Small.



PM EW&C Priorities

To support a 2028 Multi-Domain Operations capable force, designed to counter near-peer adversaries.

- **Build New Programs, *Near to Mid-Term (FY20-28)***
  - Terrestrial Layer System *
  - Joint Common Access Platform
  - Cyber Warfare Battalion *
- **Execute Current Programs, *Near to Mid-Term (FY20-28)***
  - Electronic Warfare Planning and Management Tool (EWPMT) – Capability Drop 4
  - Multifunction Electronic Warfare – Air (Large) – Flight demo and Phase 2 *
  - Prophet Modernization (ESP)
  - Tactical Space Superiority
- **Deliver Capability Now, *Near Term (FY20-22)***
  - USAREUR & CEMA Operational Needs Statement (ONS) Fielding
  - MODI and CREW to Pace Threat, reconstitute single manager role
  - Provide capabilities aligned to EW force structure growth and pacing the near peer threat
- **Set Conditions for the Future, *Mid to Far-Term (FY23-34)***
  - Cross-portfolio integration with the convergence of Electronic Warfare, Cyber, and Signals Intelligence
  - Terrestrial Layer System – Echelons Above Brigade (FY22)
  - EWPMT Increment 2 (EMBM); Maturation and Implementation of EW&C CMOSS & Photon
  - MFEW Rotary Wing and MFEW Air Small

The Electronic Warfare Planning and Management Tool (EWPMT) CD3

**First EW&C CMOSS implementations*

Distribution Statement A: Approved for Public Release. Distribution is Unlimited.

The second panel addressed Cyber at the Tactical Edge and featured COL Finch, along with **Colonel John Transue, Director of Army Capability Manager for Cyber (ACM Cyber)** at TRADOC, and **Mr. Mark A. “Al” Mollenkopf, SES, Science Advisor, Acting Chief Technology Officer, Army Cyber Command**. To begin, COL Finch reiterated the need for the Army to adapt to change – to adapt, innovate and win under new and changing conditions. To accomplish this goal, the Army is moving forward with the C5ISR/EW Modular Open Suite of Standards (CMOSS). CMOSS is being included in and managed under the SOSA initiative with the Army, Air Force, Navy, and industry participation. Specifically, it will reduce integration costs and risks, mitigate obsolescence, facilitate interoperability, and accelerate fielding and delivery of new capabilities in response to evolving threats. From a programmatic perspective, COL Finch discussed Tactical Cyber Equipment – CMOSS Chassis (TCE-CC). This program features a common chassis that supports multiple radiohead types as needed by the CMOSS cards, including Cyber/RF, GPP/Storage, and EW cards, and generic SDRs for SW based waveforms.

Mr. Mollenkopf followed by discussing how Army Cyber Command is tacking the challenge of building and sustaining complex IT systems for expeditionary and large-scale organizational use. The key to solving this challenge is improving vendor and stakeholder collaboration to ensure a accurately replicated view of the operational environment, which contributes to integration challenges. The Army is actively bringing together partners from the S&T community, service components, FFRDCs and industry to operate on the Army’s software development platform, which reduces the time it take to analyze a requirement and get new capabilities in the hands of soldiers. COL Transue closed the panel by discribing how ACM Cyber is expanding cyber capabilities from cyber mission force down to the tactical layers. Specifically, COL Transue discussed the 915th Cyber Warfare Battalion (CWB), which activated at Fort Gordon last year and includes Expeditionary Cyber Teams (ECTs), and the Army’s Intelligence, Information, Cyber EW, and SIGINT (I2CEWS) teams. He reiterated the critical role that TLS-ECB and TCE-CC will play in carrying out the cyber mission throughout the Army by delivering both offensive and defensive cyber capabilities.

For more information on any of the above presentation and topics, please contact Ken Miller, AOC Director of Advocacy and Outreach at kmiller@crows.org.

Overview of Army EW Programs

The Army is in the midst of a persistent modernization campaign to recapitalize and upgrade current systems and create an expedited path for insertion of new technology and sensors. Army CEMA covers a broad array of programs under PEO IEW&S, but major program priorities fall under the PM EW&C. The following is an overview of key programs, new and current, that AOC is closely monitoring.

Terrestrial Layer Sytem

What You Need to Know: Terrestrial Layer System (TLS) is the Army's next generation tactical vehicle-based system that delivers an integrated suite of Signals Intelligence (SIGINT), Electronic Warfare (EW), and Cyberspace Operations capabilities which will be fielded with the Army's Brigade Combat Teams (BCTs). TLS will provide the warfighters with improved situational awareness through detection, identification, location, exploitation, and disruption of enemy signals of interest. The TLS will replace both the Tactical EW Systems (TEWS) and the AN/MLQ-44A Prophet. The Army is funding two prototypes awarded to Digital Receiver Technology, Inc, a subsidiary of The Boeing Corporation, and Lockheed Martin Corporation.

On the Horizon: TLS achieved Milestone A in the Spring of 2020. OTA Prototype, Integration and Assessments are currently underway. FUE is planned for FY 2022. Another variant, TLS Echelons Above Brigade (TLS EAB) will follow with a final RFP and OTA solicitation by 3rd quarter 2021, with first unit equipped (FUE) planned during the 1st Quarter 2024.

By the Numbers: The Army requested $8.1 million for FY 2021 to support long lead components for the TLS-Large. The House Defense Appropriations Act provided $0 claiming "early to need" justification. The Senate has not released its version of the defense spending bill. For FY 2022-2025, the Army budget calls for the following:

Resource	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
Quantity	**-**	**7**	**13**	**24**	**24**
Gross/Weapon Cost	**$8.1m**	**$39.7m**	**$88.1m**	**$167.1m**	**$186.4m**

Business Opportunity: Starting in the first quarter of FY 2021, the Army will be releasing a $20-30 million contracting opportunity for maintenance and sustainment of government-owned software (Photon) for the TLS. By the 3rd quarter of FY 2022, the Army will be seeking a sustainment services and systems integration contract worth up to $1.1 billion.

Prophet Enhanced

What You Need to Know: Prophet Enhanced (PE) is an organic ground-based sensor system that can provide dedicated, all-weather, 24/7 tactical Signals Intelligence (SIGINT) and

Electronic Warfare Support (ES). Developed and supported by General Dynamics Missions Systems, the program uses Government and Commercial Off-the-Shelf (GOTS/COTS) technology to provide next generation SIGINT capabilities to keep pace with near peer and emerging threats. The PE system detects, identifies, and locates enemy emitters through multiple configurations supporting Manpack, Vehicle-Mounted, and Dismounted / Fixed-site operations.

On the Horizon: Funding for PE in FY 2021 and beyond is divided into two categories: (1) Special Purpose Systems, including support for the integration and standardization of Signals of Interest (SOI) and other improvements to address the evolving threat signal base; and (2) PE Modifications, including the fielding, training, hardware and software sustainment and other support activities from prior year procurement. Procurement of PE concluded in FY 2020. Funding for integration and standardization (Category 1) will end after FY 2021, leaving only funding for PE modifications (Category 2) in the FYDP. $61.5 million was requested for Overseas Contingency Operations (OCO) in FY 2021.

Budget Overview: For FY 2021, the Army requested $28.6 million for PE. The House Defense Appropriations Act added an additional $37 million for the TEWS.

Resource	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
Special Purpose Systems	**$11.4m**	**$0m**	**$0m**	**$0m**	**$0m**
PE Mods	**$17.1m**	**$4.1m**	**$4.1m**	**$4.2m**	**$6.7m**
Total	**$28.5m**	**$4.1m**	**$4.1m**	**$4.2m**	**$6.7m**

Multi-Function EW – Air (MFEW-Air)

What You Need to Know: Multi-Function Electronic Warfare–Air Large (MFEW-AL) is a capability set that will provide BCT Commanders with an organic airborne offensive EW capability.

MFEW-AL is a single, self-contained, airborne EW pod which will be mounted onto Gray Eagle (GE) Unmanned Aircraft Systems (UAS). MFEW-AL is based on Software-Defined Radio (SDR) Digital Radio Frequency Memory (DRFM) architecture, which will utilize both pre-programmed signal characteristic information and real-time battlefield information to complete the intended mission. MFEW-AL will be interoperable with EWPMT to support C2.

On the Horizon: MFEW-AL is scheduled to reach Milestone C in FY 2021 with full rate production (FRP) and FUE in FY 2022. Lockheed Martin Rotary and Mission Systems (LM RMS) is the OEM/Contractor. Two other iterations, MFEW-Air/Small and MFEW-Air/Rotary Wing are also on the horizon, but with few formal details at this time.

Budget Overview: MFEW-AL is a new procurement start in FY 2021. The Army requested $8.7 million for one system produced by Lockheed Martin. Over the FYDP, the Army plans to provide $58.4 million for MFEW systems. RDT&E funding for engineering and manufacturing development (EMD) activities, including 4 EMD articles, platform integration and developmental testing, is found PE 0604270A Electronic Warfare Development. The congressional House Defense Appropriations bill recommended a cut of $3.4 million to MFEW for RDT&E due to developmental test flight being "ahead of need."

Resource	Account	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	Total
MFEW - AL	Procurement	$8.7m	$19.3m	$20.1m	$10.3m	--	$58.4m
MFEW EMD	RDT&E	$45.8m	$9m	$4.5m	$5.7m	$6.7m	$71.7m

EW Planning and Management Tool (EW PMT)

What You Need to Know: EWPMT is the Commander's software to control, manage, and visualize threats in the EMS. Along with MFEW and TLS, EW PMT is pillar to the Army ability to achieve EMS Superiority. Specifically, EWPMT enables the planning and execution of EW and cyber attacks, and for the necessary assessment of those attacks, including offensive and defense EW, targeting an EM maneuvering, and cross-domain SIGINT and ISR integration. EW PMT is a Raytheon product and is an Automated Information System (AIS) following an evolutionary acquisition strategy using successive capability drops (CDs). The program is scheduled for CD 4 in FY 2021, which provides for EW Effectiveness, Enhanced Targeting, Remote Control and Management (RCM) of assets, Battle Damage Assessment (BDA), and Command Post Computing Environment (CPCE) Convergence.

Budget Overview: The Army requested $7.8 million in procurement for new equipment training (NET) Interim Contract Support (ICS) and Program Management Support. Additionally, the Army plans for $14.4 million in RDT&E (0604270A) to continue CD4, allow for participation in Soldier Touch Points (STPs) events and evaluations to the maximum extent possible, and fund Increment 1 testing and support activities for the EWPMT program.

Account	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	Total to Complete
Procurement	$7.8m	$0.8m	--	--	--	$8.6m
RDT&E	$14.4m	$17m	$2m	0	$5.9m	$39.3m

Dismounted ECM (MODI) / CREW

What You Need to Know: The Army has several systems that provide both mounted and dismounted EW capabilities to protect soldiers against Radio-Controlled Improvised Explosive Devices (RCIEDs) and radio frequency (RF) transmission threats. Many of these programs are Quick Reaction Capabilities (QRC) – point solutions fielded in a hurry to address specific threats to current operations. While the QRC route has provided some game-changing capability to the Army, it is not an optimal path to follow for sustaining and upgrading equipment. Too often, QRCs are impaired by unprepared supply chains, unreliable funding and integration with existing C4 and EW equipment. As the Army pivots away from asymmetric warfare to multiple theater operation against peer competitors, the Army is dedicated to easing the transition of these QRC to keep pace with emerging EMS threats.

MODI is a dismounted portable, programmable man-pack system that provides full spectrum coverage to maneuver so warfighters receive increased protection against RCIEDs. It is designed to counter an array of diverse threats by providing innovative offensive and defensive countermeasure capabilities.

CREW/Duke systems protect ground forces operating in convoys, single vehicle operations, or fixed locations from RCIEDs by blocking or jamming RF signals used to trigger Improvised Explosive Devices (IEDs). The Duke family of systems supports U.S. and coalition operations worldwide. CREW Duke enables spectrum dominance to protect vehicle convoys. It is used in both mounted and fixed site configurations, as well as for other non-CREW applications to include GATOR V3 and Sabre Fury. The Duke V5 is the reset version of the legacy Duke V3 Program of Record that has increased jamming effectiveness against certain threats and improves reliability and maintainability.

Baldr provides dismounted soldier level protection against RCIEDs. As another QRC Counter-RCIED EW (CREW) system, Baldr augments the Thor III force protection system and provides additional defense against RF transmission threats. Thor III is also a dismounted man-pack system that is a replacement to the Navy-procured Guardian dismounted CREW system. Baldr provides squad level protection to counter against RCIEDs. Both Baldr and Thor III are made by Sierra Nevada Corporation.

Ground Auto-Targeting Observation/Reactive (GATOR) is a system, provides fixed site organic Electronic Support (ES) and Electronic Attack (EA) to jam specific enemy transmissions. It provides increased organic Electronic Warfare (EW) capabilities at the tactical level, designed to be interoperable with CREW and the C4ISR infrastructure. The OEM for GATOR is SRC, Inc, while the sustainment contractor is CSRA, Inc.

Finally, the **Universal Test Set (UTS)** provides CREW personnel with a quick and effective field-level diagnostic capability to assess the performance of Counter-RCIED systems. Produced by Textron, the. The UTS is a Component Major Item to each of the Army developed CREW systems (Duke, Thor III, Modi, and Baldr).

Budget Overview: In FY 2021 the Army requested only $2.2 million to support the continued development of CREW (PE 0604270A) and will remain consistent through FY 2025 to fund hardware and software solutions for the system.

Resource	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	Total
CREW	$2.2m	$2.2m	$2.1m	$2.16m	$1.6m	$10.2m

Joint Common Access Platform and Tactical Cyber Equipment

What You Need to Know: The Army is slated to provide the joint force via US Cyber Command its JCAP program, a new start offensive cyber operations program of record, which will connect cyber operators across the force and synchronize efforts to target and deliver cyber effects against known threats.

Additionally, the Tactical Cyber Equipment (TCE) initiative will enable the 915th Cyber Warfare Battalion (CWB) to deliver a broad range of cyber effects in support of CEMA operations. A key component of this portfolio is the adoption of Modular Open Systems Approaches (MOSA) through development and conversion of capabilities to comply with the Electronic Warfare & Cyber C4ISR/EW Modular Open Suite of Standards (EW&C CMOSS). Initial CMOSS compliant platforms the TCE CMOSS Chassis (TCE-CC), MFEW-AL, and TLS.

RF Interference Mitigation (RIM)

What You Need to Know: RIM maintains communications capabilities in the presence of friendly and adversary Electronic Warfare (EW) systems. RIM Interference Cancellation solutions provide advantages over legacy filter-based solutions for congested and contested electromagnetic environments. Interference Cancellation (IC) Light provides a dedicated voice channel for SINCGARS during friendly and enemy jamming/interference. Likewise, IC Heavy provides a dedicated voice channel for UHF/SATCOM during friendly and enemy jamming/interference.

Tactical Electronic Warfare System/Light (TEWS/ TEWL)

What You Need to Know: TEWS is an all-weather ground tactical EW system that enables the BCT to detect, locate, identify, and counter a broad range of SIGINT activity. TEWS will integrate with current and future Army capabilities, including MFEW-Air, EW PMT and Offensive Cyber systems. TEWL is the TEWS equivalent for light BCT formations using the lightweight Flyer 72 ground vehicle. Both systems are products of General Dynamics Mission Systems.

Army EW and SIGINT Market Overview

Over the past several years, the Army has dedicated itself to modernizing its EW and SIGINT capabilities and delivering agile, adaptive, and integrated solutions to its soldiers to keep pace with the advancing threat. Additionally, as previously noted, the Army is undergoing a pivot from asymmetric warfare to multiple theater operations against peer competitors. To help balance the often competing demands of upgrading existing systems while modernizing and delivering next generation capabilities, the Army is pursuing modular open systems architecture (MOSA), specifically its C5ISR/EW Modular Open Suite of Standards (CMOSS). Many EW and SIGINT systems use the same technologies, but they are not always compatible. MOSA investments increase competition and prevent vendor lock, in which a single contractor dominates a program throughout its life cycle due to proprietary technology. CMOSS will help to adapt new technologies and address new threats as they emerge. CMOSS is initially planned for hosting on Joint Common Access Platform (JCAP) and Tactical Cyber Equipment (TCE), Terrestrial Layer System (TLS), and Multi-Function EW (MFEW) systems. CMOSS is included in and being managed by the SOSA initiative with Army, Navy, and Air Force industry participation.

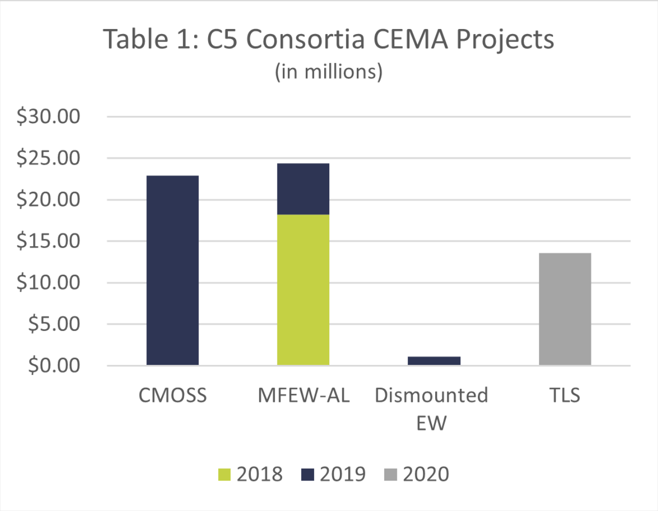


Table 1: C5 Consortia CEMA Projects
(in millions)

The use of Other Transaction Authorities (OTAs) to accelerate prototyping and fielding of new programs and capabilities adds a dimension to gauging the EW market in the US. According to Bloomberg Government, OTA contract spending is on the rise. While FY 2020 will see a slight decrease in OTA spending, undoubtedly due to the effects of the COVID pandemic, there is an expectation that OTAs will continue to be an avenue of choice to circumvent the traditional acquisition process and associated lengthy timelines. Furthermore, of the military services, the Army spends more using OTAs than the other services combined. Army OTA spending grew by $2 billion if FY 2019 to nearly $5 billion. An important note to keep in mind is that 60 percent of OTA contracts run through consortia, including the C5 and SOSA Consortia. In fact, since 2018, the C5 Consortia has awarded approximately $66 million for CEMA-related projects (see Table 1).

Most of the relevant EW and SIGINT programs and contract obligations are housed under the Program Executive Office for Intelligence, Electronic Warfare, and Sensors (PEO IEW&S), including the Program Manager for EW and Cyber (PM EW&C), PM Aircraft Survivability Equipment (PM ASE), and PM for Tactical Exploitation of National Capabilities (PM TENCAP). For FY 2020, ending on September 30, PEO IEW&S is expected to have $2.1 billion in contract obligations, up from $1.9 billion in FY 2019. Approximately one-third of the contract obligations in FY 2020 went to technical and engineering support ($684 million), while $241 million was devoted to Systems Development. The forecast for FY 2021 is up to $2.31 billion (see Table 2).

More specifically, the AOC monitors activities within 36 PE accounts spanning both

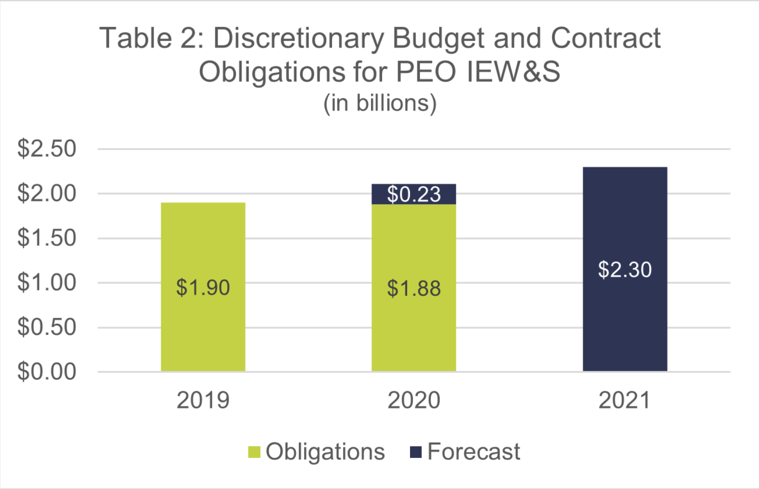


Table 2: Discretionary Budget and Contract Obligations for PEO IEW&S
(in billions)

Procurement and **RDT&E** for Army EW, Cyber and SIGINT. Within these accounts, searching keywords in program descriptions, there are as many as total of 375 activities valued at an estimated $23.4 billion in FY 21, including $10.6 billion in procurement and $10.9 billion in RDT&E. The remainder of value is distributed in other budget activity titles. Table 3 shows the value of these programs over the course of the FYDP. A significant challenge in understanding the EW market is that there is no uniform definition of what programs, activities, and capabilities comprise the market. This becomes even more difficult when considering the emergence multi-function systems

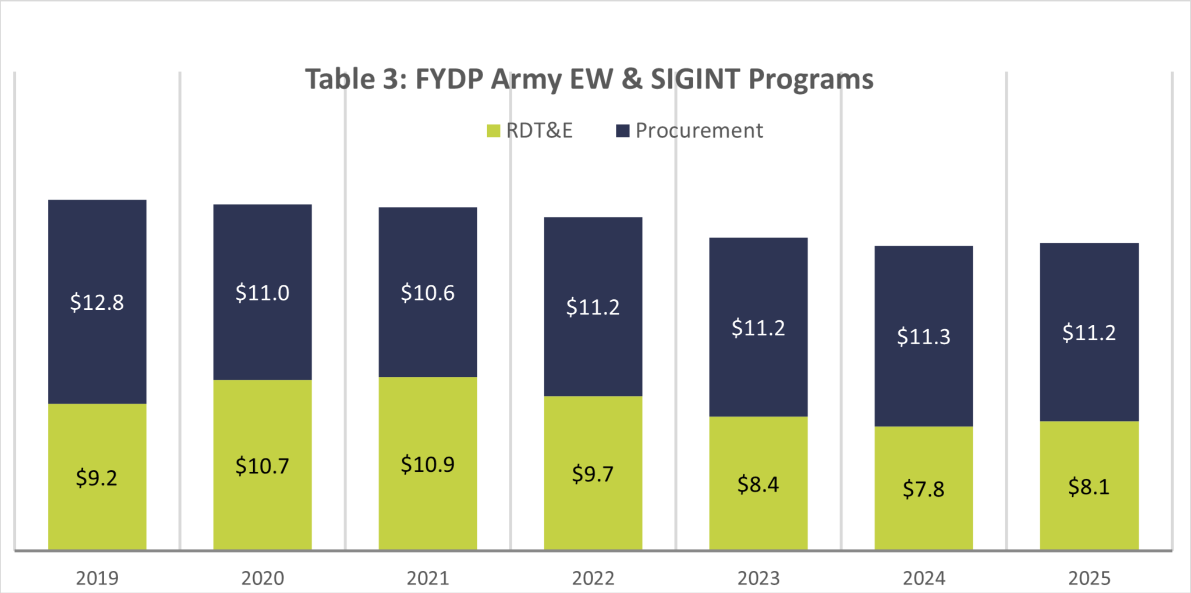
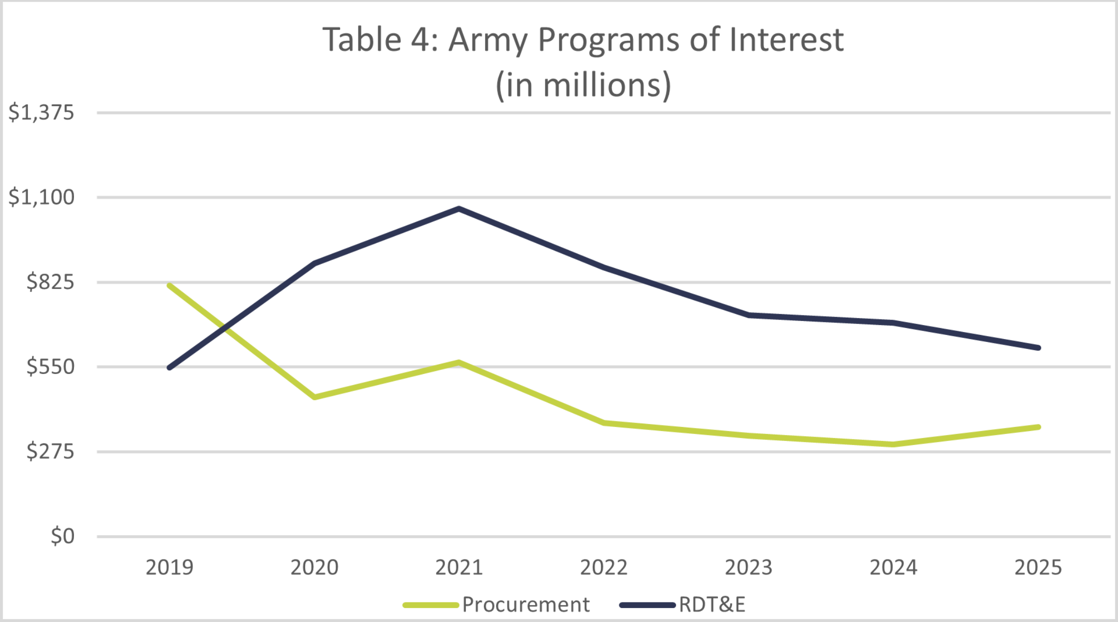


Table 3: FYDP Army EW & SIGINT Programs

In 2020, the Army spent $1.34 billion on programs that the AOC is tracking. That amount is expected to increase in FY 2021 to $1.63 billion before gradually decreasing across the remainder of the FYDP (Table 4).

In conclusion, while the Army is positioned to invest heavily in specific CEMA-related programs discussed above, including TLS, EW PMT, JCAP, TCE, and PE, overall spending on EW and SIGINT programs looks to decline slightly across the FYDP. There are at least two key reasons for this decline: (1) the Army is moving on from costly QRC programs that are not sustainable; and (2) the Army is focusing on cost-efficient, open architecture that enables cross-portfolio integration. OTAs will continue to be a priority contract vehicle to accelerate development and fielding of new capabilities.

As AOC continues to research budget and contract trends for CEMA activities and expands coverage to the other military services, we will update all information accordingly. Most of the



data above is derived from FY 2021 Army budget documentation and Bloomberg Government. All sources are available upon request. If you have any questions or need additional information, please contact Ken Miller, Director of Advocacy and Outreach, at **kmiller@crows.org**.

AOC Issue Brief:
Non-Kinetic Warfare in the Modern Digital Battlespace

(Note: The following AOC Advocacy Issue Brief was prepared by Booz Allen Hamilton, a Premier Industry Solutions Partner for the AOC CEMAlite Virtual Summit.)

The world in which the U.S. can assume ownership of the best technology, knowing its high-tech approach to war confers a unique advantage, has ended. Competing nations now also have access to critical information and cutting-edge technology, often at low cost, and are moving fast to mature and connect digital assets. The U.S. must move faster—using new ways to integrate technologies and, in doing so, ensure that they are secure, open, agile, and smart.

The rise of the internet has revolutionized warfare through a "network of networks" architecture and the data links that support it have radically increased the ubiquity and velocity of data. The strategic edge inevitably began to move to speed: harnessing information and converting it to action faster than the adversary.

Regaining the Technological Edge

As adversaries grow closer to technological parity with the U.S., national policy is refocusing on the challenges posed by its most powerful geographical foes. In 2018, the U.S. National Defense Strategy stated that our military's advantage is eroding. Declaring that inter-state strategic competition, not countering terrorism, is now our primary national security concern, DoD is setting a new priority: regaining the military's technological edge.

As the U.S.'s fight against terrorism focused on conventional operations in which the U.S. could rely on its technology edge, near-peers have evolved their ability to wage an information-centric fight. The technology underlying these information advances is sophisticated and often commercially available—enhanced with private-sector innovations—allowing these competitors to easily and cheaply disrupt existing systems. Because of this, even small states and terrorist organizations can stage cyber attacks, conduct electronic warfare, and use low-cost solutions such as drones to inform their operations or deliver munitions.

The battle is now waged over establishing and maintaining superior information as the lifeblood of all other military operations. And the U.S. must find new ways to achieve and maintain this advantage.

Challenges to Information Superiority

In thinking about how to train, equip, and staff forces for this battle over information, DoD has evolved the concept of information warfare. DoD has set an imperative of maintaining information superiority, allowing the U.S. to "collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." (Source: Joint Chiefs of Staff)

However, the U.S. faces challenges to achieving information superiority—some technical, some organizational, including:

1. **The Fragile Information Chain**: Current military systems rely on data networks, including sensor inputs, communications, computing, and so on, creating absolute reliance on a chain of uninterrupted data availability and exchange. If the information chain is broken, or simply delayed by enough time, the systems don't work. These complex systems are vulnerable to disruption, sometimes with little effort.

2. **Lack of True Connectedness**: The ubiquitous data interchange needed in modern war is hampered by the inability of many separate systems to work together, seamlessly and in real time. While some networking of weapon systems has been achieved, it's only been with great difficulty and cost. "Intra" connectedness—within, say, one service or technical ecosystem—is not enough. The goal is to have "inter"-connectedness across all systems, devices, and nodes.

3. **Proprietary Designs**: The speed of conflict, added to the pace of change by the U.S.'s adversaries, demands the ability to rapidly adapt and evolve fielded systems. The closed design practices of many original equipment manufacturers and their resulting proprietary systems and application programming interfaces (API) make this a difficult and expensive proposition. This also makes the goal of interconnectedness more difficult to achieve.

4. **Hardware-Centered Acquisition**: Traditional buying practices are focused on discrete systems and hardware and often emphasize a low tolerance for risk. And innovation (within the U.S. and without) is outpacing DoD's procurement process.

5. **Data Overload**: The practical inability to handle the flood of information being produced by all the devices and sensors on the modern battlefield is well documented. In the future, this already intractable challenge will become insurmountable without revolutionary thinking now.

Incremental change is no longer enough to advance the mission. The U.S. must pursue a new approach for the future of national defense.

A New Approach to National Defense

Information warfare is essential for meeting the challenges of near-peer conflict and DoD needs to incorporate this concept into an all-encompassing vision to comprehensively prepare for the future of war. That vision must include an information-driven, fully integrated conflict space extending across all warfighting domains, which will transcend today's organizational and acquisition boundaries. It must assume that superiority depends on critical networks—communications; intelligence; positioning, navigation, and timing; and equipment—working together even in cyber-challenged, denied, or degraded environments. And it must recognize that information is all-pervasive and is, in fact, the central organizing feature for requirements creation, acquisition, and planning and operations across the force generation lifecycle—from how warfighters are equipped and trained to how they execute in battle.

This is in contrast to information warfare, which has led to strategic moves to align non-kinetic capabilities—cyber; intelligence, surveillance, and reconnaissance; electronic warfare—in coordinated commands but still results in a siloed organization. Information and physical operators remain separated in the absence of a larger vision that drives the entire DoD enterprise to organize itself around information superiority.

That larger vision would be best mastered with acquisitions designed around information challenges rather than hardware and software to be pieced together after fielding. It would require such advances as complete data interconnectedness based on open architectures designed to speed upgrades and adaptability, and ubiquitous use of artificial intelligence (AI) at the edge. These, in turn, require far more than consolidation of commands, as they have implications for the design and data requirements of nearly every system in the force. And once achieved, they create entirely new possibilities for tactical operations in every domain.

The drawbacks of proprietary designs can also be dealt with upfront when acquisition is directed toward optimizing the entire information ecosystem. This approach would allow warfighters, combat vehicles, ships, planes, and autonomous assets to access information securely and use it to make fast, informed decisions—functioning independently, yet in coordination—to advance the mission with increased lethality. In addition, it would also lead to highly resilient systems, unprecedented agility in evolving capabilities against new threats, and breakthrough technology applications. Ultimately, thinking from this more holistic vision will help the U.S. to prevail against near-peer challengers.

Recommendations

Large, complex systems requiring lengthy development and upgrade times need to be replaced with innovative, agile technologies and solutions. DoD needs systems designed to be open, smart, resilient, and secure, and capable of operating at the tactical edge. Moving forward, DoD should focus on implementing the following central attributes into warfighting capabilities:

1. **Open:** Proprietary architectures can’t accommodate rapid upgrade cycles. DoD’s data must be taken out of proprietary silos so information that flows between the wide array of devices in the battlespace—from sensors in drones to heads-up displays on warfighters to GPS receivers—can be fully connected and integrated. Private-sector technology provides ways to construct open frameworks so that:
   - Components and software modules can be switched in and out to fulfill rapidly changing requirements, missions, battlefield conditions, and tech advances.
   - Technologies are interoperable and plug-and-play.
   - Open architectures, data platforms, and APIs are understandable, usable, and accessible to facilitate data integration.

2. **Smart**: Information must be delivered as intelligence giving warfighters real-time context for the precise mission and situation. Yet data is pouring in faster than military and national security operations can analyze it, requiring new thinking to aggressively triage the data and quiet the noise. New computing paradigms need to be rapidly incorporated:
   - Machine learning (ML) and other forms of AI, trained and continuously refined, can accomplish routine tasks and substantially aid humans in resolving critical ones.
   - Developers must integrate data science expertise with in-depth mission and domain knowledge to achieve mission success.

3. **At the Edge:** Traditional communications channels and networks can be jammed or otherwise denied, which can impede command and control; processing, exploitation, and dissemination of intelligence; and situational awareness. Military systems need new capabilities to operate at the edge:
   - Networks and processing must be resilient against electronic warfare attack or other disruption.
   - Systems must operate without a cloud or network, empowering the user with increased situational awareness and real-time decision making.
   - To quickly develop systems that are agile and cost- effective, we must create ecosystems using smart devices already in the field.

4. **Resilient and Secure:** Open platforms, ML, AI, and edge processing and networks are being subjected to increasingly sophisticated cyber attacks and other electronic threats. Adversaries have invested heavily in emerging technologies and can disrupt these networks using cheap, commercially available equipment.
   - DoD must embed advanced cyber protection into solutions as they are developed, rather than bolted on later.
   - Cybersecurity must be continually refined and updated through agile processes.
   - Data scientists must work with machines, augmenting human expertise with advanced AI, to protect algorithmic models from spoofing and other attacks.

To learn more about this topic, visit BoozAllen.com/DigitalBattlespace.

Booz | Allen | Hamilton®