AOC ADVOCACY

AOC ISSUE REPORT

THE EVOLUTION OF US ARMY SIGNALS INTELLIGENCE (SIGINT)

Written by AOC Staff

EXECUTIVE SUMMARY

"The fundamental problem at hand is this: Army SIGINT must evolve its organizations, training, equipment, and doctrine to ensure our readiness to provide timely and relevant SIGINT to support the Commander's information needs in large-scale combat operations against a sophisticated adversary." - LTG Scott Berrier

On July 18, 2018, the Association of Old Crows' (AOC) SIGINT Industry Partnership Project (IPP) held **"Winning the Electromagnetic Spectrum (EMS): The Future of Army SIGINT,"** a two-part event comprised of a congressional panel discussion and Industry Solutions Forum (ISF), on Capitol Hill. The panel, hosted by Rep. Jody Hice (GA-10), featured LTG Scott Berrier, Deputy Chief of Staff (G-2), LTG Stephen Fogarty, Commanding General, Army Cyber Command, MG Robert Walters, Commanding General, Intelligence Center of Excellence, BG Jennifer Buckner, HDQA, DCS G-3/5/7, Director, DAMO-CY, and Mr. Alex Cochran, Senior Cryptologic Advisor, US Army Intelligence and Security Command. The panelists discussed the then-newly released Army SIGINT Strategy and efforts to integrate SIGINT, Electronic Warfare (EW), and Cyber.

Mr. Kevin Sherman, SES, Office of the Undersecretary of Defense for Intelligence (OUSD[I]), Military Intelligence Program Resources, gave his thoughts on the discussion at the ISF immediately following the panel. He spoke on the need for a mix of low-end and high-end intelligence, surveillance, and reconnaissance (ISR) systems to maintain a competitive edge against peer and near-peer competitors. His remarks were followed by a showcase of SIGINT technologies from IPP Partners and exhibiting companies.

"Winning the EMS" was convened to showcase the evolution of Army SIGINT and its integration with EW and Cyber Operations (CO). The Army's recently released SIGINT Strategy is an important step to charting the future of its Cyber Electromagnetic Activities (CEMA) concept as it responds to a range of dynamic threats in an increasingly complex Electromagnetic Operating Environment (EMOE).

During the Cold War, SIGINT was initially used to track an adversary's position and intentions. As time went on, the Army realized the advantages of employing SIGINT and EW battalions to assist division commanders. These battalions were successfully used through the end of the Cold War. In the 1990s, Army SIGINT continued to focus on traditional communications collection and jamming but even though there was no easily-identifiable peer adversary against

which to deploy these SIGINT battalions. Thus, the Army struggled to develop new SIGINT technologies and it was not until the end of the decade that a new SIGINT program was finally fielded. The attacks on 9/11 caused a major shift in SIGINT operations to targeting and intercepting in civilian and commercial environments. These environments were typically the domain of intelligence agencies; now the Army was having to employ its soldiers to use these same techniques on the battlefield.

The post-9/11 landscape also led to the rise of improvised explosive devices (IEDs) which spurred the Army to start re-employing EW assets alongside SIGINT assets. However, this was not the more robust EW/SIGINT integration visible today; EW was evolving outside of the Army SIGINT realm, not within it. It was not until 2010 that initial steps were taken to further integrate the two, along with the newly identified Cyber domain. The Army created a new operational concept, CEMA, that bridged Cyber and EW, creating an Electromagnetic Spectrum Operations (EMSO) oriented plan for its future force. The new CEMA concept did not immediately impact the Army SIGINT community, but it did advance the conversation. In recent years, the Army has taken a closer look at how it fights in the EMS by providing more SIGINT support to lower echelon units, that eventually culminated in the publication of the 2018 Army SIGINT Strategy.

The Army SIGINT Strategy calls for four Lines of Effort (LOE): building and organizing an Army SIGINT force; training, managing, and investing in the force; equipping the force; and developing a SIGINT doctrine. To achieve these objectives, Army leadership is prioritizing the ongoing integration of SIGINT, EW, and CO. The commitment to this effort was shown at the July 2018 AOC SIGINT IPP event, where leadership from the different “tribes” all spoke of working together and breaking down barriers between them.

BACKGROUND AND HISTORY OF US ARMY SIGINT

COLD WAR

During the Cold War, when the US Army was focused primarily on defending Western Europe against an attack by Warsaw Pact land forces, SIGINT played an important role in monitoring enemy movements and providing indications and warning to corps commanders. As the Army shifted its thinking from “active defense” in the 1950s and 1960s to the more aggressive Air- Land Battle concept in the 1970s and 1980s, it needed intelligence and EW forces that could maneuver more effectively and support the needs of division commanders.[1] The Army decided to tailor some if its military intelligence battalions into combat EW and intelligence (CEWI) battalions in order to provide its combat divisions with “organic” SIGINT and communications EW capabilities.[2] A typical CEWI battalion could provide communications electronic attack, SIGINT, and other types of reconnaissance to the division. The Army also fielded CEWI brigades at the Corps level.

[1] Kelly, Maj. Patrick J, US Army, “The Electronic Pivot of Maneuver: The Military Intelligence Battalion,” published by the School of Advanced Military Studies, US Army Command and General Staff College (Fort Leavenworth, KS) (http://www.dtic.mil/dtic/tr/fulltext/u2/a264449.pdf), 1993.

[2] Clarke, Tricia M., “What Might Be the 2025 Equivalent of the 1980s CEWI Battalion,” in Small Wars Journal (http://smallwarsjournal.com/jrnl/art/what-might-be-the-2025-equivalent-of-a-1980s-cewi-battalion).

1990s

The CEWI concept proved to be very successful during the 1991 Gulf War. However, with the end of the Cold War and a waning focus on near-peer adversaries, the Army gradually abandoned the CEWI concept during the 1990s. However, communications jamming remained important to Army SIGINT operations throughout decade. Military intelligence battalions would use high-power communications jammers, such as the AN/TRQ-32 Teammate and AN/TLQ-17A TrafficJam, to deny enemy communications across operationally significant portions of the EMOE. By leaving a few frequencies clear of jamming, the enemy would migrate communications to these frequencies, making it much easier for Army SIGINT operators to monitor and locate them.

During the 1990s, the Army struggled to define new SIGINT requirements –identifying the right mix between ground and airborne collection assets to support division and brigade commanders and field new EW and SIGINT systems. The Intelligence and Electronic Warfare Common Sensor (IEWCS) program was slated to provide a family of organic networked ground-based EW and SIGINT systems. However, the program was cancelled in the 1997-98 timeframe because the technology was already outdated.

2000s

In the wake of the IEWCS program cancellation, the Army began a more modest Prophet program in 1999 and eventually fielded several variants of communications intelligence (COMINT) and electronic attack systems to support regular Army brigades and Army National Guard units.

During the early 2000s, the Army began development of the Aerial Common Sensor, a multi-sensor aircraft (including a robust SIGINT capability) that was to replace the RC-12 Guardrail SIGINT aircraft and the RC-7 Airborne Reconnaissance Low multi-INT aircraft. However, the program ran into a variety of technical challenges and was cancelled, restarted and cancelled again.

After the 9/11 attacks, operations in Afghanistan and Iraq reshaped Army SIGINT operations, especially in terms of the types of targets and signals that the Army needed to collect. These new requirements focused on targets that lived among the civilian population and whose communications hid in the vast commercial electromagnetic environment that previously the Army had no concerns about monitoring. The SIGINT policy had to be tailored to enable Army SIGINT platforms to monitor and collect signals from commercial communications devices (a mission previously handled mostly by the NSA). This was not a difficult target set from a technology aspect, but the volume of signals traffic from commercial networks was much larger than anything the Army had encountered before.

By 2006, the growing presence of remote-controlled improvised explosive devices (RCIEDs) in Afghanistan and Iraq pushed the Army to re-establish a dedicated EW enterprise to

handle this new, high-priority threat. This development created new requirements for tactical EW systems, such as RCIED jammers, which were mounted in ground vehicles and later worn by soldiers. A number of the Army's new tactical EW developments were taking shape outside the scope of the SIGINT community with the integration of high-power electronic attack and SIGINT systems, such as Prophet Enhanced.

2010s

In the 2007-2010 timeframe, the Army began to focus on cyberspace as an operational domain. As cyber-based systems became more dependent on the EMS (the transition from "wired" computing to "wireless" systems), the Army began in 2010-2011 to articulate a new operational concept, CEMA, that spans Cyberspace and the Electromagnetic Spectrum. CEMA seeks to leverage the operational synergies between EW, cyberspace operations and spectrum management from a man, train, and equip perspective. The Army's focus on CEMA has led it to reorganize its former EW enterprise within its larger Cyber enterprise, and within organizations such as the Cyber Center of Excellence at Fort Gordon, GA.

RECENT DEVELOPMENTS

"The threat's increasingly advanced radars tied to long range air defenses and fire support systems require the Army to emphasize Electronic Intelligence (ELINT) — not just to support the Army, but to ensure our Joint Services can penetrate tough Anti-Access Area Denial (A2/AD) environments to set the conditions for close combat on the ground."

In July 2018, the AOC's SIGINT IPP organized an event, **"Winning the EMS: The Future of Army SIGINT,"** on Capitol Hill. The first session featured an Army leadership panel hosted by Rep. Jody Hice (GA-10). An AOC Industry Solutions Forum immediately followed, including a keynote conversation with Mr. Kevin Sherman, SES, OUSD(I), Military Intelligence Program Resources. The panel discussed the emerging progress that the Army is making to integrate SIGINT, EW, and CO, fueled by a rapidly changing operational environment that requires a pivot from an emphasis on counterinsurgency operations (COIN) to a multi-domain battle against peer and near-peer competitors. This transition guided the Army to produce a new SIGINT strategy that calls for the synchronous pursuit of four major objectives.

According to LTG Berrier, "Our SIGINT way ahead will not only enable the Army's Electronic Warfare and Cyber initiatives, it will also form an indispensable foundation from which our EW and Cyber warriors will seize the initiative and dominate our adversaries within the electromagnetic spectrum." The Strategy supports the Commander's need to see, aggregate and understand increasingly complex electromagnetic operating environments across multiple domains, blending adversary, civilian and blue force activities, and enable decisive action to deliver effects, often simultaneously and collaboratively, against a target.

For the Army to achieve this end state, SIGINT needs to be better integrated with Army operations as a whole, and one of the primary avenues to accomplish this is for SIGINT to support CEMA operations. The Strategy spells out four essential LOEs that enable this objective. The first LOE necessary for this integration is to organize and build a SIGINT force that not only maintains its mastery in locating, identifying and tracking threats with accuracy and precision, but attains the same level of mastery as it applies to complex RF signatures from emitters in the EMOE. LTG Fogarty, Commanding General, Army Cyber Command, shared that this LOE is already underway and bearing results as the Army is committed to spending $1 billion over the next four years to build a world-class Cyber school on a new campus at Ft. Gordon, GA. At this new school, soldiers will be trained in EW, Cyber and SIGINT operations. This learning environment is the first of its kind to teach skills from all three competencies at one location. It is a fundamental building block to prepare the SIGINT Force of tomorrow to support EW and CO.

Army SIGINT Leadership Panel

LTG Scott Berrier, Deputy Chief of Staff (G-2)
LTG Stephen Fogarty, Commanding General, ARCYBER
MG Robert Walters, Commanding General, ICOE
MG Jennifer Buckner, HDQA, DCS G-3/5/7, Director, DAMO-CY
Alex Cochran, Senior Cryptologic Advisor, US Army INSCOM

SIGINT Strategy LOEs

1. Organize and Build the SIGINT Force
2. Train, Educate, and Manage the SIGINT Force
3. Equip the Army SIGINT Force
4. Develop SIGINT Doctrine and Messaging

The second LOE is to “Train, Educate, and Manage the SIGINT Force,” which advances an Army SIGINT Enterprise with robust capabilities, but also the depth and breadth of a well-trained and adaptable team of warfighters across all three disciplines. Today, the Army SIGINT force lacks sufficient training and knowledge to conduct integrated SIGINT operations against peer and near-peer competitors in large-scale operations. Furthermore, military intelligence leadership cannot consistently integrate SIGINT with the other disciplines. LTG Fogarty highlighted that the current operational tempo is accelerating the learning curve, but also providing valuable lessons to answer these challenges. To guide this effort, the Army is leaning on several elements, including the Military Intelligence Training Strategy - a published set of standards and activities for non-Intelligence commanders to objectively train Intelligence soldiers, augmented with the new Intelligence, Electronic Warfare Tactical Proficiency Trainer (IEWTPT), and re-establishing the Technical Control and Analysis Element (TCAE) to elevate the quality and integrity of information collected by Army SIGINT forces.

The third LOE is to “Equip the Army SIGINT Force,” which focuses on two challenges. First, the Army needs systems that can infiltrate and operate in contested EM environments, especially aerial ISR assets. LTG Berrier noted, “The threat’s increasingly advanced radars tied to long range air defenses and fire support systems require the Army to emphasize Electronic Intelligence (ELINT), not just to support the Army, but to ensure our Joint Services can penetrate tough Anti-Access Area Denial (A2/AD) environments to set the conditions for close combat on the ground.” Second, rapid technology advancements and adversary use of

commercial-off-the-shelf technologies challenge the Army's ability to adapt quickly. The acquisition process throughout the Department of Defense is simply too slow to keep pace with advances in technology and the adversary decision cycle. The Army not only needs new collection capabilities, but also engineering solutions to upgrade existing systems in the field rapidly. While the Army has a Rapid Capability Office (RCO) and is working to provide solutions to the entire force, its SIGINT Enterprise has not taken full advantage of this process.

An important area of progress is in the Terrestrial Layer Intelligence System (TLIS), which is pursuing a survivable and tactically relevant capability to the Army, which as LTG Berrier stated, "sustains connectivity to the broader national SIGINT enterprise." To continue progress and address challenges associated with this LOE, both BG Buckner and MG Walters noted that stable and secure funding is essential to keep pace with the development of core enabling technologies, especially the use of Artificial Intelligence (AI) and Machine Learning (ML) across data collection, processing, exploitation and dissemination. Through this next generation of technology, the Army will deploy SIGINT/EW/Cyber on single platforms, both on the ground and in the air. The family of sensors fulfilling these missions must have an increased frequency range to locate, collect and exploit signals.

Finally, the fourth LOE is to "Develop SIGINT Doctrine and Messaging". In late 2017, the Army rewrote Field Manual 3.0 to close a capability gap in conducting sustained, large-scale combat operations. Army SIGINT Doctrine will reflect the full integration of SIGINT, EW, and CO and provide a new generation of intelligence soldiers capable of employing their skills effectively in multi-domain operations. Furthermore, the Capability Development and Integration Division at Ft. Huachuca is working closely with the Army Capabilities Integration Center (ARCIC)/Army Training and Doctrine Command (TRADOC) to develop concepts and requirements that will drive future capabilities consistent with the complex EMOE.

This closer relationship between SIGINT, EW and CO will drive materiel decisions, such as multi-function systems that feature all three capabilities and provide new potent capabilities to the Army.

ANALYSIS

The SIGINT Strategy is an important step for the Army to integrate SIGINT into its broader CEMA construct. As the Army continues to move from strategy to operational planning and normalized execution, it may evolve into a robust EMSO-oriented model for the other Services and our allies.

The Army is taking a logical approach by integrating SIGINT to support CEMA operations. Despite some acquisition setbacks in the 1990s and 2000s, The Army has done a fairly good job of maintaining its ground-based and airborne SIGINT capabilities, through programs such as Prophet Enhanced and the RC-12 Guardrail, despite some acquisition setbacks. These and other Army SIGINT systems typically perform the same functions (emitter detection, location and identification) that communications EW systems perform. Therefore, it is important to leverage the information gleaned from SIGINT operations with other EW activities to help build a better

operational picture of the EM environment for exploitation by the tactical operations centers (TOCs).

Another important aspect of integrating SIGINT with CEMA operations is that SIGINT assets will provide more support to lower echelon units in addition to their customers at division and corps. This contributes to the operational objective of making capabilities available to commanders on the ground, which results in more lethal and better protected units.

The LOEs contained in the Army SIGINT strategy will continue to drive changes across doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF). This is a significant change in the approach the Army has conducted EW and SIGINT operations over the past 20 years. It shares a similar methodology and range of operational benefits that CEWI provided in the final decades of the Cold War.

"Our adversaries, and their associated proxies are either already using or will soon be capable of employing RF-agile software defined radios and sophisticated commercial communications equipment in a contested electronic environment which will challenge our current collection systems."

The Army has spent a significant amount of time and effort to encourage the respective SIGINT, EW and Cyber communities to work together in a synergistic fashion under CEMA. One of the keys to success of this concept will be to strike the right balance between leveraging SIGINT, EW and Cyber capabilities effectively while supporting the individual development of each of these disciplines. The long-term challenge for the Army will be to ensure that SIGINT, EW and CO requirements are each properly resourced and do not compete with one another.

CONCLUSION

"I think that you'll also find that our SIGINT way ahead will not only enable the Army's Electronic Warfare and Cyber initiatives, it will also form an indispensable foundation from which our EW and Cyber warriors will seize the initiative and dominate our adversaries within the electromagnetic spectrum."

The new Army SIGINT Strategy represents major progress in a Service-wide effort to close gaps identified as the Army transitions from "a COIN-centric SIGINT support apparatus to an integrated SIGINT/ EW /CO capability supporting multi-domain operations against peer and near-peer adversaries and win our nation's wars." SIGINT operations are now contributing to CEMA with respect to emitter detection, location, and identification. The concept of integrating SIGINT, EW, and CO is driving changes among Army personnel development, such as soldiers who are trained across all three disciplines. Personnel with SIGINT, EW, and CO expertise will reside in TOCs, shortening the time it takes to make decisions and take action with regard to EMS or cyberspace operations. Additionally, Army training will need to prepare soldiers for operations in congested and contested electromagnetic environments.

It is important to note that the SIGINT Strategy LOEs require a unity of effort across the Army, which in turn requires a change in culture. Cultural change is a function of leadership, learning, and implementation over time. The Army leadership and unity of message represented at the SIGINT IPP event was a positive sign that the Army is moving in the right direction. Furthermore, as LTG Fogarty reiterated, there is sense of urgency that is motivating this change and accelerating the learning curve. The complexity of the threat has revealed itself to the operational force, which is resulting in wide-spread agreement about the necessary outcomes of this new strategy. As progress continues, the Army must normalize integrated SIGINT, EW, CO operations through realistic training, joint exercises, and ongoing missions.

INDUSTRY SOLUTIONS FORUM

Following the congressional panel discussion, the AOC hosted an ISF to showcase how industry leaders are responding to the technological challenges facing the Army SIGINT Enterprise. Mr. Kevin Sherman, OUSD(I), provided the keynote address. In his remarks, Sherman stressed that China and Russia have been gaining ground in the SIGINT/EW/CO field. They have improved their capabilities since the end of the Cold War, when the U.S. turned its attention to COIN operations and tactics.

The concern over Chinese and Russian technological advances is highlighted in the 2018 National Defense Strategy (NDS). The NDS states that the U.S. needs to focus on the threat from peer and near-peer adversaries. The goals laid out are to improve lethality and readiness to combat these growing threats. According to Sherman, industry will need to reflect the verbiage in the NDS in their Request for Proposal (RFP) responses. Prioritizing the goals of the NDS will be key to obtaining funding, while failure to do so could lead to missed opportunities. The Army SIGINT Strategy aligns with the current NDS, which has been firmly pushed to all levels of the DoD.

He concluded his remarks by saying that intelligence operations are being shaped by an increasingly congested and contested battlespace. To maintain our superiority, we must do two things. First, we must improve our EW capabilities to protect the battlespace and our assets in it. Second, we need to collect intelligence on the capabilities of our adversaries, identify gaps, and exploit them. This is where industry has the opportunity to develop innovative solutions for the future fight. He sees the need for a mix of low and high end ISR to maintain our competitive edge and developed with simplicity in mind. The DoD is ready and waiting for these capabilities; all industry needs to do is answer the call.

DISCUSSION QUESTIONS

On the surface, the Army's concept of providing greater SIGINT support to CEMA operations makes sense; however, it also poses several challenges that will need to be addressed in greater detail. Have a question to advance the SIGINT IPP discussion? Email Ken Miller, Director of Advocacy and Outreach, at **kmiller@crows.org**.

1. What does the Army's new SIGINT strategy mean for the development of future EW and SIGINT systems, such as TLIS and MFEW Ground? How will Army acquisition officials manage the legal partition between Title 10 and Title 50 activities with respect to combined tactical EW and SIGINT systems?

2. Where will the Army's offensive communications electronic attack activities fall under the CEMA concept? Will some be retained exclusively to support SIGINT operations? If so, will there be a centralized acquisition authority and user community?

3. Now that many of the Army's EMS-related activities (Cyber operations, EW, spectrum management and SIGINT) are aligned (or at least, in the case of SIGINT, being coordinated) via CEMA, what does this mean for the Army's CEMA doctrine, and more generally, the Cyberspace Warfighting Domain? Is this a further step by the Army toward establishing a new Information-Based Warfighting Domain?

4. The Army has articulated a SIGINT strategy in which tactical SIGINT assets will support CEMA operations. Is there an opportunity for CEMA operations to support tactical SIGINT collection? Could tactical EW systems that are deployed closer to the frontline help by detecting low-power emitters and cueing SIGINT sensors?

ABOUT THE AOC

The Association of Old Crows is an organization for individuals who have common interests in Electronic Warfare (EW), Electromagnetic Spectrum Management Operations (EMSO), Cyber Electromagnetic Activities (CEMA), Information Operations (IO), and other information related capabilities. The Association of Old Crows 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. For more information, visit **crows.org**.

The views expressed in this report are for discussion purposes only and do not necessarily reflect the views of the AOC, its members, or SIGINT IPP Partners. The AOC will update this report periodically as developments warrant.

The AOC would like to thank Warrior Support Solutions for contributing to this report. If you have a question or comment, please contact Mr. Ken Miller, Director of Advocacy and Outreach at **kmiller@crows.org**.

THE AOC WOULD LIKE TO THANK OUR SIGINT IPP PARTNERS FOR MAKING THIS EVENT POSSIBLE.

BAE SYSTEMS

Headquartered in Arlington, Virginia, BAE Systems, Inc. employs approximately 32,000 in the United States, United Kingdom, Sweden, and Israel, and generated 2016 sales of $10 billion. BAE Systems, Inc. provides support and service solutions for current and future defense, intelligence, and civilian systems; designs, develops and manufactures a wide range of electronic systems and subsystems for both military and commercial applications; produces specialized security and protection products; and designs, develops, produces, and provides service support of armored combat vehicles, artillery systems, and munitions.

Darkblade Systems

Darkblade Systems is a Service-Disabled Veteran-Owned Small Business (SDVOSB) providing scientific, engineering, technical, operational support, and training services to Federal government and Commercial clients. Engineering specialties include development and design services for hardware and software systems fulfilling the mission needs of the Department of Defense and Intelligence Communities. Operational and Cyber services include full spectrum project and program support, including planning, training, management, and technical evaluation.

Raytheon

Raytheon Company is a technology and innovation leader specializing in defense, civil government and cybersecurity solutions. Founded in 1922, Raytheon provides state-of-the-art electronics, mission systems integration, C5I™ products and services, sensing, effects and mission support services. Raytheon is headquartered in Waltham, Massachusetts.

L3

L3 Technologies is an agile innovator and leading provider of global ISR, communications and electronic systems for military, homeland security and commercial aviation customers. L3 develops advanced defense technologies and commercial solutions in pilot training, aviation security, night vision and EO/IR, weapons, maritime systems and space.

KEYSIGHT TECHNOLOGIES

Keysight Technologies Inc. (NYSE: KEYS) is the world's leading electronic measurement company, transforming today's measurement experience through innovations in wireless, modular, and software solutions. With its Hewlett-Packard and Agilent legacy, Keysight delivers solutions in wireless communications, aerospace and defense and semiconductor markets with world-class platforms, software and consistent measurement science. The company's nearly 12,600 employees serve customers in more than 100 countries.

PERSISTENT SYSTEMS

Persistent Systems offers a secure and scalable mobile networking capability based on its cutting-edge Wave Relay MANET Technology. Persistent's products provide a total solution consisting of voice, video, and situational awareness to mobile users with no reliance on fixed infrastructure. For more than a decade, Persistent has been a pioneer in developing advanced MANET technology and commercializing it in the Defense and Industrial sectors.

HARRIS

Harris Corporation is a leading technology innovator, solving customers' toughest mission-critical challenges by providing solutions that connect, inform and protect. Harris supports government and commercial customers in more than 100 countries and has approximately $6 billion in annual revenue. The company is organized into three business segments: Communication Systems, Electronic Systems and Space and Intelligence Systems. Learn more at harris.com.

IN ADDITION, THE AOC WOULD LIKE TO THANK THE FOLLOWING COMPANIES WHO EXHIBITED AT THE INDUSTRY SOLUTIONS FORUM

The team at Epiq Solutions has extensive experience tackling real-world signal processing challenges for our customers. We can design and deliver world-class hardware, software, and system solutions to meet your mission-critical signal processing needs. Our staff can handle stand-alone projects from start to finish, where we are wholly responsible for a design and implementation of a solution. We can also work as a trusted partner to supplement an existing development team.

NASK is a provider of leading edge digital signal processing solutions that are deployed on all platforms: ground, vehicle, air-borne, and space. We have a full catalog that includes an assortment of existing EW/SIGINT/Force Protection capabilities and solutions, all of which can be tailored to meet the unique needs of our customers. We have a full Research and Development team that embraces the exploration of new technologies. NASK is a mission driven company where meeting customer require-ments comes first.

Motorola Solutions provides SDR platforms that access intelligence feeds across spectrum to increase situational awareness and real-time intelligence. Technology that will transform your missions into smaller footprints and change the way you run your operations. There is no longer any need to carry multiple pieces of equipment. We offer one-box-solutions that adapt to multiple mission types. Combined with tailored applications, your personnel will be more nimble, have real-time data for faster deci-sion-making and improve mission efficiencies. Small form factors providing warfighters the freedom of movement by land, sea and air. Look to Motorola Solutions for modern battlefield solutions.