Army White Paper

The Army Science Board
"Electronic Warfare (EW) in Peer Deterrence and Conflict"

Observations of the Ad Hoc Team
Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Subcommittee

20 August 2024

The Army Science Board

Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology

Headquarters, Department of the Army

Foreword

The Army Science Board (ASB) is chartered under the Federal Advisory Committee Act (FACA) to provide the Army with independent advice and recommendations on matters relating to the Army's scientific, technological, manufacturing, acquisition, logistics and business management functions, as well as other matters the Secretary of the Army deems important to the Department of the Army. ASB members and consultants are dedicated experts who volunteer their time to provide independent assessments to Army civilian and military leaders.

In September 2023, the ASB began preliminary data gathering on the Army's capabilities to conduct Electronic Warfare (EW) against peer adversaries. The work was conducted under the auspices of the ASB's Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Subcommittee. The effort evolved into a prospective FY24 study titled "EW in Peer Deterrence and Conflict," with the purpose to address likely challenges the Army would face in the USINDOPACOM Theater during competition, deterrence, and conflict. In May of 2024, the Army elected not to sponsor a full study on this topic.

During the 8 months of data gathering, significant interactions with stakeholders across the Army, industry, and DoD provided a clear picture of the direction the EW community is headed, the emerging threats, the current state of technology, and the likely pace and direction of technology maturation in the 2030 timeframe. The observations collected from that data gathering process are presented in this paper.

The following white paper is a product of the ASB. The statements, opinions, observations, and conclusions contained herein are those of the ASB study members and do not necessarily reflect the official position of the Army or the Department of Defense. The contents of this white paper have not been discussed, adjudicated, or formally adopted by the Parent Board and are solely intended to provide the Secretary with an independent assessment on the Army's operational EW capabilities.

Michael E. Williamson
Chairman
Army Science Board

Contents

INTRODUCTION

The Army's current EW capabilities developed over the past two decades of fighting counterinsurgency operations. During that time, the Army became increasingly reliant upon readily accessible national, sister service, and intelligence community resources. As near-peer adversary capabilities have emerged, the demand for these resources has grown. Army 2030 will not experience the same level of access for its EW capabilities, most notably as it takes more of a supporting role in the USINDOPACOM Theater. To continue meeting U.S. national security objectives and protecting national interests in theater, the Army must gauge how it provides effective EW deterrence and attack capabilities, and how it will adopt those capabilities to meet projected requirements through 2030.

To begin assessing the Army's capabilities, the ASB C5ISR Subcommittee established an ad hoc team to conduct preliminary research and data gathering. The Army did not request a full study to be conducted, therefore the ad hoc team did not complete thorough analyses under more specified terms of reference.

The ad hoc team conducted 8 visitations across the country and met with over 30 Army, Sister Service, U.S. Government, FFRDC, industry, and academic stakeholders in the EW community (see Appendix B). Based on the data gathered, the team made the following primary observations:

1. Despite the criticality of EW to the effectiveness of every phase of military operations, particularly in the INDOPACOM theater, there is no executive agent or proponent designated at the highest level of the Army to ensure appropriate resourcing of critical functions, equipment, training, and staffing.

2. The People's Republic of China People's Liberation Army (PLA) space capabilities closely match or exceed those of U.S. Army Pacific (USARPAC). The PLA would likely use space capabilities to exert command and control of their forces offshore, and that activity would offer a key preamble to an invasion or other efforts to reclaim Taiwan. These capabilities are also essential to target beyond the first island chain. Continued investment is required to deny the PLA its capabilities to use BLOS for command and control.

3. System timing (Positioning, Navigation and Timing (PNT)-derived or other) is a key element of EW systems and adversaries are intent in denying the U.S. ability to use precision weapons by denying precise timing sources necessary for enabling the communications system on which those weapons depend. Every critical system needs to be M-Code compliant or have alternative PNT capabilities.

4. The Army makes operational and resourcing decisions based on analytical data that supports value to the warfighter, but its EW discipline lacks this analysis capability:

    a. The Army requires actual threat-based EW modeling and simulation capabilities to

estimate the effectiveness of operations in advance of execution and in training. The tools necessary to accomplish this in the electromagnetic spectrum (EMS) arena do not exist at the scale and fidelity to properly address the requirements.

b. The Army should identify and prioritize EA investments based on careful operational and quantitative system analysis of the most important adversary kill chains that joint commanders seek to break. The analysis should include an assessment of other non-EA capabilities that could be developed/employed, so that EA resources can be directed especially towards developing capabilities where no other options exist.

5. The Army has not hardened its mission command, air and missile defense, and long-range precision fires systems to protect them from enemy jamming.

6. Effective Army EMS capabilities will require increased EW and space manning, cleared billets, and the associated training and equipment for the EW mission.

More granular observations are provided below, presented to reflect doctrine in FM 3-12, "Cyberspace and Electromagnetic Warfare," and categorized as falling under EA (electronic attack), EP (electronic protection), or ES (electronic warfare support).

The ad hoc team sought to understand the Army's role in providing the Joint Force with EW capabilities, specifically assigned to the U.S. Army Pacific (USARPAC) in the USINDOPACOM area of responsibility (AOR). Its review of the role of EW in the current USINDOPACOM operational plan (OPLAN), with a focus on the Army's responsibilities, was threat-informed, and the baseline operational context used by the team follows.

OPERATIONAL CONTEXT

Engagements with leaders and senior staff in the Indo-Pacific and input from other visits by the ad hoc team suggested the scope and scale PLA capability across all domains, kinetic and non-kinetic, presents a challenge, if not overmatch, to U.S. forces forward in theater and those can reasonably deploy into theater in the early stages of conflict. Should conflict come, combat is expected to last months with significant losses suffered by both sides.

The PLA has seen substantial growth–several orders of magnitude–in key areas. Its growth is a product of the largest buildup of military forces since WWII, fueled by consistent increases in defense spending, including a 7% real increase last year. Most PLA capabilities relevant to conflict with the U.S. are recently acquired, technologically sophisticated, benefiting from leading edge technology, and fielded in large numbers. For example, thousands of missiles and aircraft (albeit fewer 5th generation aircraft), and hundreds of ships, many performing at or exceeding key aspects of U.S. capability. Consequently, the PLA has advantages in range, magazine depth, proximity, and interior lines to support and enable their force.

These advantages are particularly evident with PLA capabilities to wage war in the EMS–putting at risk the U.S. Joint, networked, precision way of war. The PRC and its army demonstrated the importance placed on information superiority with the recent creation of its information warfare command. It places a premium on command-and-control warfare, focused on denying the U.S. and its allies key capabilities including (1) the ability to network forces; (2) accessing signals from space for warning, intelligence, command and control, and targeting; and (3) the information and warning generated from its space, aerial, and terrestrial sensor, and sensor to shooter networks.

The PLA's strategy was made clear in its 2006 "Science of Campaigns," with information power the first of five essential elements of campaign strength. The "Science of Campaigns" states its armed forces must pursue information superiority {youshi} and continuously strengthen its own information strengths before being able to put itself in an invincible position in future wars. In the document, EW refers to a comprehensive capability for protecting one's own unimpeded employment of the EMS and disrupting the enemy's employment of the EMS, an important component of information power {xinxili}. It includes the capabilities for electronic reconnaissance and counter-reconnaissance, jamming and counter-jamming, and destruction and counter-destruction. In a modern campaign, the position and roles of EW capability increase daily; electronic confrontation {dianzi duikang} activities will be jointly conducted by multi-service electronic confrontation force-units and penetrate operations from beginning to end. Not only is the confrontation broad in range, large in both scale and space, the means and modes of confrontation have trended toward diversification. The strengths or weaknesses of EW capability have become an important indicator for balancing operational effectiveness of campaign strengths.

The PLA has robust EW capabilities at every echelon across all its forces and in its joint force. EW capabilities have seen significant growth as well, particularly in those forces most relevant to conflict in the South China Sea. The capabilities are aimed at denying communications and countering/jamming U.S. and allied sensors, systems, command and control, and PNT. Training and proficiency remain unclear, but China has studied Russian EW successes and failures and are

adjusting accordingly.

Conversely, U.S. Army capabilities are more responsive to the needs of USEUCOM and are not relevant given the scope and scale of the PLA threat and the ranges at which that threat can operate. As with many other aspects of the military balance, U.S. Army and Joint EW forces in the Indo-Pacific are outnumbered, outranged, and outpowered by those possessed by the PLA.

This capability imbalance puts at risk several missions, functions, and weapon systems, including communications, maneuver, targeting, command and control, early warning, surveillance, electronic attack, EW, and PNT. Without resolution, the Army and the Joint Force risk losing freedom of action in the EMS that underpins its ability to operate and fundamental to the US way of war.

Most, if not all the Army's systems and operations depend on assured access to the EMS. Losing freedom of action in the EMS limits or loses secure communications and computer networks, determination of position, precise time and synchronization, weapons targeting and effectiveness, intelligence, and awareness and ability to deny adversaries' use of the EMS. Collectively, those losses increase U.S. and allied forces' susceptibility to anti-access and area denial regimes. Additional operational impacts include the degradation of synergies fundamental to U.S. Joint warfare that allow it to fight outnumbered and win. For example, U.S. and coalition forces would experience reduced capabilities to roll back adversary air and missile defense, to defend against and attack adversary long range fires, to penetrate enemy air space, and to integrate air-ground operations at speed and scale.

Enabling U.S. forces to successfully operate in a contested EMS environment will require Army capabilities that can sense the EMS at depth, and EW systems and capabilities that are expeditionary, agile, and distributed versions of larger, more powerful ground-based EW and space control systems. These need to be employed at speed (warning is likely measured in days, not weeks and months), scale (hundreds of manned and unmanned EA, EP and ES systems), range (measured 1000's of kilometers, not 10's or 100's), and duration to disrupt PLA command and control, mission networks, force generation, force application, sensors, and fires and targeting signals.

Finally, most if not all, of the PLA's long-range weapons, targeting, and command and control are as dependent on the EMS as U.S. forces. Denying the PLA access to the EMS falls to the Army. Navy and Air Force EW/EMSO are force-focused, enabling fleet and force package employment and operations that generate pulsed (non-continuous) operations that do not provide the persistence needed to deny the EMS to the PLA and deliver durable, consequential effects. Properly enabled, only the Army can generate persistent, adversary-focused EW/EMSO at the scale and duration necessary to deny access to the signals that run through the EMS on which the PLA depend to operate. Like "owning the night," owning the EMS and denying the EMS to the adversary is imperative. Current EW capabilities are inadequate in number, range, and power, and key weapons platforms depend on the EMS and need to be hardened now.

OBSERVATIONS

The following observations are presented to reflect doctrine in FM 3-12, "Cyberspace and Electromagnetic Warfare," and are categorized under Electronic Attack (EA), Electronic Protection (EP), or Electronic Warfare Support (ES). The ad hoc team also made theater-specific and spectrum management observations, an identified cross-cutting issues for consideration by the Army.

Electronic Attack

- The Army should identify and prioritize EA investments based on careful operational and quantitative system analysis of the most important adversary kill chains that Joint commanders seek to break. Analyses should include an assessment of other, non-EA capabilities that could be developed and employed so that EA resources can be directed towards developing capabilities where no other options exist.

- Incorporating deception tactics and innovative EW techniques can enhance operational effectiveness and confuse adversaries. Obfuscation of ongoing Army operations related to maneuver, deployment, logistics, or repair activities present a significant challenge. Given the geographic limitations for land operations in the Indo-Pacific theater, the development of these techniques carries greater importance. Although other kinetic means can protect ground assets from attack, a robust signal disruption and deception needs to form part of the defense concept.

  - Continued research and development in these areas is necessary for the Army to maintain a tactical edge. This includes exploring new methods of signal obfuscation, decoys, and misdirection to disrupt enemy operations. Coordinating research, development, testing, and evaluation (RDTE) efforts across services can help address immediate technology gaps to rapidly field effective countermeasures against adversary sensor systems.

  - The Navy has invested heavily in the underlying technology and is well ahead. The Army and Marines may benefit from the Navy efforts, but only in certain limited scenarios in which case specific Synthetic Aperture Radar-Moving Target Indication (SAR-MTI) offshoots may be an appropriate short-term strategy to make headway on technology availability by 2030.

- The Army needs the ability to position EW capabilities in austere areas without supporting infrastructure, such as ports, airfields, etc. These systems will be minimally manned or unmanned. Army systems, including those under development today, are large, require significant infrastructure and are manpower intensive. The EW community should look specifically at remote operations or teleoperated capabilities that avoid the requirement of soldiers to operate the systems.

- Investment in rapid capabilities specifically designed to defeat specific adversarial systems should be a high priority (jamming and precision jamming within the context of a revised concept of employment in the INDOPACOM theater). Organizations that can rapidly provide

solutions (industry, FFRDC/UARCs/Labs) can provide interim solutions while the Army works towards full-scale acquisition. Force integration should be addressed simultaneously. Development of these capabilities will require collaboration with the intelligence community.

Electronic Protection

- Adversaries in the INDOPACOM AOR are developing and deploying more sophisticated jamming capabilities. Robust, jam-resistant communication systems will be critical. Advances in waveform technology will ensure reliable communications even in contested environments. This will enhance command and control, situational awareness, and overall mission success.

- The Army should increase its efforts to analyze and assess the susceptibility of its own systems to EA. Threat-informed red teaming, suitable metrics, testing and ranges to support that testing are needed. NGIC and TSMO could support this type of activity.

- Adversaries are continually improving their EW capabilities to disrupt or destroy U.S. command and control, making it a constant battle to maintain an edge. Jam-resistant waveforms will continue to mature and provide significant advantages to EP dominance. Traditional anti-jamming and low probability of intercept/detection (LPI/LPD) techniques remain important, but new strategies such as geometric discrimination offer promising avenues for advancement. Beam forming, steering, nulling and other advanced signal processing will enhance signal clarity and reduce interference.

- The Army can re-program some of its existing EP systems based on threat changes, but the process takes too long. The workflow associated with reprogramming based on threat should be revisited to find/gain efficiencies and adapt more rapidly to a changing threat.

- EP is treated separately by each program office, so EP is often not given the attention it merits. Systems used as components of the same kill chain need to have comparable levels of EP commensurate with the threat they face. Because of the distribution of EP requirements across systems (radar, PNT, comms, weapons guidance) resourcing is fragmented and reducing the EP of the overall kill chain. EP is often not updated to keep pace with the threat; resourcing needs to be provided to permit rapid EP reprogramming.

EW Support

- The proliferation of advanced sensor technologies has made traditional methods of sensor allocation and tasking obsolete. A more decentralized approach to sensor management may be necessary to fully leverage these developments. Investigating the feasibility and benefits of decentralized sensor data tasking and consumption will help optimize sensor utilization and enhance situational awareness.

Theater-Specific EW Considerations

- Contested logistics support in theater will depend on EP/EA systems operating effectively. The Army will require locations to conduct resupply and evacuation of battle-damaged material, medical evacuation, system repair and staging. Warehousing and forward deployed inventory will be under constant surveillance and threat of adversary targeting. As such, deception, cover, and kinetic support is required, some of which may take the form of electro-magnetic responses.

- While there are U.S. flagged enclaves and stationing agreements with allies, the INDOPACOM theater presents significant challenges to operations for the Army and the Marines. These include expeditionary requirements for the Army deploying capability rapidly, providing protection against electronic attack, and other operational protections.

- For certain EW effects, equipment needs to be operated in the area of interest on the ground in order to generate the desired effect. Therefore, equipment needs to be small, mobile, and survivable. While the Army can benefit by examining the Marine Corps' capabilities and concepts for expeditionary warfare in the theater, only the Army can provide the persistent effects required by the theater commander at scale.

- Given a lack of organic assets, the Army is reliant on the USAF for EW attack and support. These assets may not be available in a conflict in the Indo-Pacific theater, so the Army will need a new solution to this problem.

<u>Spectrum and EW Battle Management</u>

- Although there are EW planning systems, Army specialized command and control of EW and spectrum management is limited because there is no overarching battle management system. The Army has made various attempts over the years to develop spectrum management or battle management software inclusive of spectrum, but those efforts have fallen short. Further investment is required to address effective spectrum planning, dynamic management, and total spectrum visualization in theater (red and blue). Focus and investment in this area are necessary to achieve comprehensive spectrum awareness and control in contested environments.

- Given the nature of EW, it is difficult to ascertain battle damage assessment of systems that have been subjected to electronic attack. As such, novel techniques may be required to determine if the Army's electronic attack was effective in disabling and destroying the adversary's capability and the extent to which the adversary can return the targeted assets to service.

- Because there is no overarching battle management system for EW, it is very difficult to integrate EW with other effects. For example, within the missile defense architecture, there needs to be an exchange of information between EW planning and management and the IAMD battle management system(s). With data from an EW battle management system, engagement decisions to shoot a kinetic missile or use a non-kinetic effect could be improved. The need to

exchange information extends beyond the IAMD mission, e.g. to short, medium and long-range artillery (which employ radar and other EMS sensors).

Cross Cutting Issues

- The Army has significantly underinvested in EW, by choice, divesting and deemphasizing electromagnetic operations in prior funding cycles. Some research has continued at a modest level, but concepts or prototypes did not transition into fielded systems or new TTP's. The Army has not focused on EW threats posed by peer adversaries. Recent activities to replace aging capabilities, although technologically advanced, are poorly suited to the geography and threat environment of the INDOPACOM theater. However, there are opportunities to remedy the situation if a concerted effort is taken to repackage or preposition EW capability in theater.

- Identifying and investing in critical technologies such as advanced jamming, signal processing, and cyber-electronic warfare will be essential. These investments will help bridge the current capability gaps and ensure readiness for future challenges. Organizations that can rapidly provide solutions (industry, FFRDC/UARCs/Labs) can provide interim solutions while the Army works towards full-scale acquisition.

- While the Navy investments in EW RDTE will help advance Army developments, the Army's operational requirements are very distinct. Additional research will be required to translate from Navy to Army use cases.

- The Army needs to continue to reduce the obstacles to effective EW caused by Title 10/Title 50 policy distinctions and leverage concepts for onshore protection and signal related matters around sense, exploitation, and attack capabilities.

- Artificial intelligence (AI) offers significant potential for identifying and countering electronic attacks. In the short term, AI can automate the detection and analysis of threats, improving response times. Long-term, AI could enable more sophisticated and adaptive EW strategies, making continued investment in AI research and development essential.

  - AI can be used to identify the adversary's highly dynamic use of the EM spectrum. Ongoing efforts should continue to be funded and matured; specifically, classification efforts such as understanding zero-day signals in space and devising effective responses in near real time. Both are achievable, but will require continued investment in classifiers, robust delivery capability, and monitoring of the signal's environment. The latter requires investment in receiver technology and experimentation with AI enabled classifiers.

  - A concerted effort will be needed to collect signals intelligence for analysis and training AI models. Although the U.S. has the capability to do so, collection is done for traditional analysis methods of processing, exploitation, and dissemination without a focus on training machine learning systems.

- The Army lacks the force structure necessary to engage in effective EW warfare at the scale and range relevant to the threat. The requirements of 2030 in INDOPACOM may necessitate the development of additional specialized force structures.
  - Given the likely increasing use of AI, the Army may be required to rethink force structure, Soldier/leader competencies, and training. For example, the inclusion of data scientists, investment in high-performance computing at the tactical edge, and finding the balance between democratized and specialized EW capabilities.

- The Army should inventory the EW susceptibility and spectrum requirements of its systems, accompanied by an experimental/test campaign of learning.

- The Space domain offers many opportunities and challenges for Army operations. The Army's contribution to space control in the INDOPACOM region is unique and essential to the joint force. The Army needs more EW-focused experiments and demonstrations to understand the potential and likely risks to operations in the space domain.

  - Rationale to perform experiments in theater, given representative terrain and signals environment.

  - Infrastructure investment may be required to provide a simulated, representative signals environment for the maturity of systems and operational testing as well as individual and unit training.

- The Army uses a variety of rapid acquisition processes to develop quick reaction EW capabilities, but the mainline contracting teams who will acquire the long-term operational systems are often brought in late in the process. Sustainability and maintainability costs should not be borne by the operational unit. Budgeting and contracting organizations should have early visibility to these rapid acquisition efforts to set conditions for earlier transition to programs of record for more effective life cycle management.

APPENDIX A. TERMS OF REFERENCE

SECRETARY OF THE ARMY
WASHINGTON

02 SEP 2022

MEMORANDUM FOR Chair, Army Science Board

SUBJECT: Terms of Reference (TOR) for Army Science Board (ASB) Subcommittees

1. Based on ASB recommendations, I approve six subcommittees. The TOR for each subcommittee is enclosed and summarized below:

   a. Environmental Advisory Board (EAB) Subcommittee: Addresses engineering, construction, real estate, stability operations, and environmental management products and services as well as development of the Nation's water resources.

   b. Weapons Systems Subcommittee: Addresses rotorcraft Design Synthesis & Performance Assessment (DS&PA); ground combat vehicle DS&PA, Soldier interaction, and system integration; lethality, including impact physics, energetics, warhead DS&PA, effects modeling and simulation; survivability and protection; air & missile defense DS&PA.

   c. Basic Sciences and Enabling and Disruptive Technologies Subcommittee: Addresses basic sciences and enabling and disruptive technologies, to include Soldier performance enhancement, cognition improvement, and training; autonomous systems and human-machine teaming; Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE); Countering Weapons of Mass Destruction (CWMD); Energetics; Material science; and Emerging technologies.

   d. Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) and Digital (Information Technologies) Subcommittee: Addresses Tactical edge command, control, and communications (C3) in contested environments; Situational awareness overmatch; Information Operations (IO); Electronic Warfare (EW); Intelligence analysis processes and tools and visualization methods; and Information technologies embedded in systems.

   e. Science and Engineering Adoption, Adaption, Integration, and Sustainment/Disposal Subcommittee: Addresses Advanced physical and digital prototyping and experimentation in operational environments and advanced tools to support prototyping and experimentation; Adoption, adaption, and integration of emerging technologies into existing weapons systems; Sustainment; to include engineered resilient systems, agile logistics, and health management; Disposal of weapons systems through foreign military sales, demilitarization, and other means to better use existing resources;

Policies affecting the modernization of weapon systems and the organizations in which they are employed.

f. Intelligence and Assessment Subcommittee: Assessment of threat technical and operational capabilities and their impact on the Army; Assessment of U.S. vulnerabilities and potential mitigation approaches; Interactions/integration with the other members of the Intelligence Community including access to classified intelligence up to TOP SECRET (TS) collateral, Sensitive Compartmented Intelligence (SCI), and Special Access Programs (SAP) levels as required.

2. As authorized by the Secretary of Defense and the Secretary of the Army and pursuant to the Federal Advisory Committee Act of 1972 and Government in the Sunshine Act of 1976, the Chairman of the Army Science Board (ASB) establishes these six TORS. The subcommittees shall not advise senior Army leaders on individual Department of Defense (DoD) or Department of the Army acquisitions outside of an authorized ASB study effort, nor shall any subcommittee member be placed in the position of acting as a contracting or procurement official, which may constitute a conflict of interest. The subcommittees will provide findings and recommendations to the ASB parent board members for deliberation.

3. As per the Secretary of Defense memorandum dated August 14, 2021, each subcommittee will be comprised of no more than 15 members.

4. My point of contact is Ms. Heather J. Gerard, Executive Director, Army Science Board, at (703) 545-8652 or heather.j.gerard.civ@army.mil.

Christine E. Wormuth

6 Enc
1. EAB Subcommittee TOR
2. Weapons Systems Subcommittee TOR
3. Basic Sciences and Enabling and Disruptive Technologies Subcommittee TOR
4. C5ISR and Digital (Information Technologies) Subcommittee TOR
5. Science and Engineering Adoption, Adaption, Integration, and Sustainment/Disposal Subcommittee TOR
6. Intelligence and Assessment Subcommittee TOR

Army Science Board
Subcommittee Terms of Reference

Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) and Digital (Information Technologies) Subcommittee

1. Overview: As authorized by the Secretary of Defense and the Secretary of the Army and pursuant to the Federal Advisory Committee Act of 1972 and Government in the Sunshine Act of 1976, the Chairman of the Army Science Board (ASB) establishes the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) and Digital (Information Technologies) Subcommittee. The following Terms of Reference (TOR) outline the duties and responsibilities of the subcommittee in accordance with the ASB charter (May 2022).

2. Mission Statement: The C5ISR and Digital (Information Technologies) Subcommittee, as part of the ASB, shall address issues and assist ASB Study teams with providing advice and recommendations to the Secretary of Defense through the Secretary of the Army on matters relating to the Army's C5ISR and digital (information technologies) core competencies, including:

a. Tactical edge command, control, and communications (C3) in contested environments.

b. Situational awareness overmatch.

c. Information Operations (IO).

d. Electronic Warfare (EW).

e. Intelligence analysis processes and tools and visualization methods.

f. Information technologies embedded in systems and in Army, Joint, and ally/coalition networks.

Neither this subcommittee nor the ASB shall advise senior leaders on individual Department of Defense (DoD) or Department of the Army acquisitions, nor require any subcommittee member to be placed in the position of acting as a contracting or procurement official, which may constitute a conflict of interest.

3. Methodology: The subcommittee may incorporate and apply any of several methodologies including, but not limited to, reviews of the literature, interviews, and briefings necessary to support ASB study teams conducting work on topics related to the subcommittee's scope.

4. Tasks: The subcommittee shall support individual ASB study teams with expertise in its related fields. In addition, the subcommittee shall maintain cognizance of the Army's activities in its related fields, to include research and development, maintenance of the science and technology base, budgeting, policy, strategy, doctrine, and other factors that further the conduct of ASB study teams. At a minimum, the subcommittee will report annually to the ASB Chair on its activities.

5. Support: The Executive Director of the ASB and the Office of the Assistant Secretary of the Army for Acquisitions, Logistics, and Technology (ASA(ALT)) will provide the necessary logistical and administrative support to the subcommittee to conduct its business as assigned.

APPENDIX B. AD HOC TEAM MEMBERS

David Jimenez (Co-Chair)

Thomas Cole, BG (Ret) USA (Co-Chair)

Richard G. Ames, PhD.

Kari Anderson

Gary Blohm

Michael Dowe, Jr., PhD.

Scott Goldstein, Maj Gen (Ret) USAF, PhD.

William Guyton, Jr.

William Hix, MG (Ret) USA

Christine Michienzi, PhD

Venkat Mummalaneni, J.D.

Thomas Russell, PhD.

Fred Schneider, PhD.

Teresa Shea

Samuel Visner, PhD.

Senior Advisors

Michael Macedonia, PhD.

Teresa Smith

Marc Zissman, PhD.

APPENDIX C. DATA GATHERING (VISITATIONS)

The ad hoc team gathered data from the following organizations.

- U.S. Army Futures Command
- Georgia Tech Research Institute
- Johns Hopkins University Applied Physics Laboratory
- MIT Lincoln Laboratory
- Program Executive Office for Intelligence, Electronic Warfare & Sensors
- Program Executive Office for Command, Control and Communications-Tactical
- U.S. Army Combat Capabilities Development Command
- United States Army Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (formerly CERDEC)
- U.S. Army Communications-Electronics Command
- Naval Research Labs
- U.S. Army Pacific
- Assistant Secretary of the Army (Acquisition, Logistics and Technology)
- National Ground Intelligence Center
- U.S. Army Test and Evaluation Command
- Army Research Laboratory
- Defense Ammunition Center
- Deputy Under Secretary of the Army
- U.S. Army Cyber Command
- Deputy Chief of Staff G-2
- United States Army Intelligence and Security Command
- U.S. Marine Corps Forces, Pacific