AY 2022-2023

ELECTROMAGNETIC WARFARE ROADBLOCKS: STIFLING INNOVATION AND OPERATIONAL EFFECTIVENESS

ELECTROMAGNETIC WARFARE INDUSTRY STUDY

GROUP PAPER

COL TRAVIS RUHL, INSTRUCTOR

SEMINAR #1

**The Dwight D. Eisenhower School
for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062**

Table of Contents

Executive Summary

The United States must innovate and operationalize electromagnetic warfare (EW) capability across the electromagnetic spectrum (EMS) or U.S. national security will be at risk. Superiority in the EMS maneuver space is a fundamental precursor that enables the Department of Defense (DoD) to successfully operate in all domains and achieve the goals of the National Defense Strategy. The ability to operate freely within the EMS – at the time, place, and parameters of the nation's choosing – is no longer guaranteed within today's geopolitical environment. While acute threats like Russia pose significant EMS threats, the People's Republic of China (PRC) presents the United States with its most significant pacing challenge. China fuses innovation across civil and military spheres, which enables it to make technological advances quickly. To maintain EMS superiority, the United States must remove roadblocks and impediments that slow EW innovation and prevent EW operational effectiveness.

During the 2022-2023 academic year, twelve field grade officers and civilians attending National Defense University's Eisenhower School of National Security and Resource Strategy examined impediments to EW innovation and barriers to translating innovation into EW operational effectiveness. They examined the EW ecosystem across the triple helix of government, industry, and academia and developed resourced recommendations for the DoD's consideration to bolster innovation and accelerate operational effectiveness.

This paper addresses six areas that could be improved to boost EW innovation:

- **Leadership**: lack of EW operational expertise and misaligned authorities
- **Data science**: lack of data scientists and data standardization
- **Open system architecture:** implications for innovation and new technology adoption
- **Classification:** the barriers created by over-classification that prevent collaboration
- **Domestic demand signals:** the implications of the industry's inability to access classified EW data coupled with the DoD's failure to provide clear EW demand signals
- **International collaboration**: impediments to allied interoperability and shared innovation

Innovative systems and processes are only helpful if they can be translated into operational effects. This paper also addresses four areas that could be improved to enhance EW operational effectiveness:

- **Doctrinal alignment:** EW needs to be clearly defined and integrated into joint capstone and keystone documents to provide consistent guidance across the joint forces
- **Electromagnetic spectrum management:** commercial interests are often in conflict with DoD operational requirements for EMS planning and real-time spectrum management
- **Realistic EW training:** operators at all levels need EW system training, but training options must mitigate adversary opportunities to observe and exploit U.S. capabilities
- **Data sharing:** the electronic warfare integrated reprogramming (EWIR) process must move at an operationally relevant pace, and new methods for data sharing can help

Ultimately, the U.S. EW ecosystem evolved out of decades of direct investment as well as growth in related and supporting industries, and it is meeting military's current needs. But in order to maintain EMS superiority in the future, the DoD must remove the roadblocks identified in this paper and continue to critically examine the U.S. EW ecosystem to maintain collaboration, creativity, innovation, and operational effectiveness in the future.

The State of EW Today and the Vision for Tomorrow

"Future combat will be less about the capability of individual weapon systems and more about how a network of systems communicate and work together through the use of the electromagnetic spectrum."[1]

– Former Congressman Jim Langevin during March 2021 Congressional Hearing

In the 2015 book *Ghost Fleet*, fictional versions of the Chinese and Russian governments launch a surprise attack on the United States.[2] They seize initial victories by using extensive cyber and electromagnetic warfare (EW) capabilities to disable global positioning system (GPS) satellites and to blind air defenses. After the EW attacks disable critical U.S. technological capabilities, the adversary's kinetic attacks were impossible to stop and extremely effective. One of the book's authors, military technologist P. W. Singer, made the near future scenario realistic enough to land the book on required reading lists across the Department of Defense (DoD).[3] Now, eight years later, the imaginary war seems more plausible than ever. Tensions between the United States and China continue to grow while China makes rapid progress in EW technologies to support their view of EW being "an integral component of modern warfare."[4] Similarly, the Russians are jamming GPS signals at this very moment to disrupt the targeting of U.S.-provided High Mobility Artillery Rocket System (HIMARS) weapon systems in Ukraine.[5] Meanwhile, the current Air Force Chief of Staff, and potential future Chairman of the Joint Chiefs of Staff,[6] has stated that the U.S. military has been "asleep at the wheel" for decades when it comes to EW.[7] The problem is clear; the DoD cannot adequately address the EW challenges it will likely face during a future conflict with China or Russia.

While the situation appears dire, the DoD has significant opportunities to advance EW innovation and operational effectiveness. <u>The United States already possesses the necessary financial resources and technology needed for EW dominance, but it lacks the organizational</u>

structure, culture, and will to use those resources to create timely, innovative EW capabilities and effectively transition those capabilities into the operational forces.

The DoD updated the term "electronic warfare" in the 2020 Joint Publication (JP) 3-85, and EW is now "electromagnetic warfare." JP 3-85 defined it as: "Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[8] U.S. joint forces must train, operate, and maneuver in this increasingly complex electromagnetic operational environment (EMOE) to establish and maintain command and control, communications, intelligence, targeting, and tracking capabilities. EW operations include electromagnetic attack (EA), electromagnetic protection (EP), and electromagnetic support (ES) as the sword, shield, and eyes respectively within U.S. electromagnetic spectrum operations (EMSO). This paper approaches EW as a key military function of joint electromagnetic spectrum operations (JEMSO) and a critical component for U.S. superiority in the electromagnetic spectrum (EMS).[9]

The first section of this paper will use a modified application of Porter's Diamond to analyze the EW defense industries and innovation ecosystem. While there are several impediments to overcome, this analysis shows that there are solutions that can be implemented to increase the DoD's EW effectiveness for the purposes of both deterrence and combat effectiveness. The second section examines how EW innovation can be accelerated by increasing leadership and EW expertise within the DoD by removing the roadblocks that currently impede collaboration across the EW ecosystem. Finally, the third section will outline how maturing technologies from accelerated innovation can enable the DoD to increase the speed and effectiveness of EW absorption into the operational forces. This absorption can be achieved through collaborative management of friendly and adversarial electromagnetic emission data as well as improved doctrine and training. The recommended changes are summarized in Appendix

4: Capstone Analysis. The DoD urgently needs to make changes to improve how it develops and employs EW capabilities, especially considering some senior DoD leaders are predicting that a conflict with China could occur by 2025[10] or 2027.[11]

Strategic Environment Related to EW

The DoD has made substantial progress in how it talks about EW in its strategic documents. The 2022 National Defense Strategy explicitly warns of China's "electronic and informational warfare capabilities"[12] and stresses the importance of partnering with NATO allies on EW platforms.[13] The 2020 Electromagnetic Spectrum Superiority Strategy (EMSSS) connects the intent of achieving EMS superiority to "military readiness, integration across warfighting domains, and increased lethality of U.S. forces."[14] The 2020 EMSSS also takes important steps to unite EW and EMS management and creates a unified vision for EMSO. The EMSSS established five broad goals to achieve a vision of freedom of action in the EMS by 2030. The goals are well crafted and achievable. But the DoD has been slow to turn that strategic vision into operational capabilities that can deter or defeat a technologically advanced adversary.

America's primary adversaries are in very different strategic situations when it comes to advancing their EW technology. Russia is exercising EW tactics and techniques daily as they wage war against Ukraine. While Russia may seem weakened by the war and U.S.-led economic sanctions, history demonstrates that operational military experience, even if unsuccessful, can strengthen a country's ability to adapt tactics and strategies to modern technology. China, as the DoD's pacing challenge,[15] "has become a serious competitor in the foundational technologies of the 21st century: artificial intelligence (AI), 5G, quantum information science, semiconductors, biotechnology, and green energy."[16] For example, Harvard's Belfer Center recently assessed that "China has already surpassed the U.S. in quantum communication and has rapidly narrowed America's lead in quantum computing."[17] These technological advancements coupled with

China's military-civil fusion and focus on offensive EW would make China a challenging foe. China's autocratic leadership and demographic decline may force China's leader Xi Jinping to focus on domestic issues, but the DoD cannot rely on the hope that an aging dictator, more concerned with his legacy than diplomacy, will choose peace over conflict.

EW Industry Analysis Through the Lens of Dual Use Technology

The DoD relies on private companies, academic institutions, government laboratories, federally funded research and development corporations (FFRDCs), and non-profit entities to develop EW systems. This section will utilize the Porter's Diamond model to conduct an analysis of how the U.S. EW ecosystem works. Michael Porter's model encompasses four attributes: 1) factor conditions, 2) demand conditions, 3) related and supporting industries, and 4) firm structure, strategy, and rivalry. Porter originally formed this model to determine how industries achieve international business success.[18]

This section will also incorporate an assessment of how and whether leveraging dual use technology is beneficial (or even possible) for EW systems. Currently, research and development (R&D) in the United States is largely funded by commercial interests, so the DoD is interested in taking advantage of those investments and utilizing commercially-developed products whenever possible. However, some mission areas may not be good candidates for adopting commercial systems.[19] For example, while there are a small number of non-military reasons for ES and EP, including border protection and law enforcement, EA is a uniquely military effect aimed at denying, disrupting, degrading, destroying, and/or deceiving an enemy's military EMS activities.[20] The commercial market provides incentives for companies to innovate in areas tangential to EW, such as autonomous cars, sensors, microelectronics, and unmanned systems, but there is little incentive for commercial companies to develop military EW systems.[21] Nonetheless, because of the ongoing improvement of related technologies, EW systems stand to benefit greatly in terms of cost and development timelines if defense companies can find ways to leverage commercially available technologies.

The first attribute in Porter's Diamond is known as factor conditions, and it refers to the key factors, such as skilled labor and infrastructure, that an industry needs to successfully innovate and produce products.[22] Advanced factors are factors that require sustained investment over time to create and are highly specialized to an industry's particular needs.[23] For the U.S. EW ecosystem, this includes the government investing in developing radar expertise as far back as World War II.[24] Other government and private investments have combined to create the highly specialized base of sensor, automation, radiofrequency (RF), and microelectronics knowledge and skills that is needed to develop EW systems. Due to the presence of government labs and academic institutions involved in related scientific research, the people with these skillsets tend to be clustered around Boston, Los Angeles, Stanford, Dayton, and the District of Columbia. In the 21st century, private investors have contributed to the development of dual use technologies like unmanned systems and AI/machine learning (ML), which are tangential to or directly supportive of the EW industry.

Furthermore, the United States fought in multiple armed conflicts in which EW played a meaningful role. Vietnam, for example, led to the development of the AN/APR-38 receiver system, which allowed the F-4G Wild Weasel to locate and home in on hostile radar signals.[25] The United States also avails itself of technology from subsidiaries of foreign companies with ongoing real-life EW battle experience, such as that gained by Israeli defense companies Rafael and Elbit. The long-term investment Israel made in EW for its own defense is a factor condition contributing to the success of the U.S. EW ecosystem since products and information flow from these companies to their U.S. subsidiaries.[26]

The second attribute is demand conditions, which covers the economic concept of consumer demand for products.[27] The military services, which operate with different requirements for different mission areas, make up the limited U.S. EW consumer base.

The demand signal for dual use technology began in 1994 when Secretary of Defense William Perry issued a memorandum that directed program managers to "rely more on the commercial marketplace."[28] Contemporaneous EW system developers pointed out that the first step to incorporating dual use parts would be foundational changes in EW system design. In particular, the industry needed to develop architectures that would allow devices from different manufacturers to function together, which is a problem that has since been largely resolved by government insistence on open system architecture standards.[29] The next set of issues that developers and the government needed to address was the fact that very small computers were not available commercially in the mid-1990s, which is a problem the market resolved due to consumer demand for ever smaller, more powerful electronics products, such as smart phones.[30]

One persistent problem with dual use technology for EW systems that the market has not yet resolved is related to the very nature of commercial products: fast-paced change equals fast-paced obsolescence.[31,32] Commercial companies have very few incentives to provide long-term sustainment for legacy products, especially for a customer like the DoD, which demands small quantities compared to the commercial market. The other persistent problem noted by past developers is the fact that COTS products are not rugged enough to operate in military environments (Figure 1).[33,34] This can be solved to a certain extent by rigorous government analysis of the real need for better-than-COTS requirements.[35] However, the military operates in challenging and non-commercial environments, and if it is not acceptable that a solution based on COTS or modified COTS products can only meet 80 percent of the DoD's requirements, then the government should be careful about its demand for dual use

Type	Original Market	Modified by DoD Before Use	Examples
Commercial off the Shelf (COTS)	Commercial	No	Office software, furniture, CCTV
Modified COTS	Commercial	Yes	Passenger aircraft, satellites buses
Government off the Shelf (GOTS)	Government/ Military	If needed prior to use with a new system	Munitions, certain EW suites

Figure 1: Dual Use Technology Categories

technology with respect to EW.[36] On the other hand, COTS-based solutions are good candidates for prototyping and rapid test-fail-fix cycles until designs are finalized.

Type	Example Organizations
Universities	MIT, Stanford, Johns Hopkins
FFRDCs	GTRI, MIT/LL, MITRE
Government Laboratories	AFRL, NRL, ARL
Non-Profits	University of Dayton Research Institute, Wright Brothers Institute, STR

Figure 2: Non-Commercial Supporting Organizations

The third attribute in the Porter's Diamond model is related and supporting industries, and it refers to the grouping of supplier companies and other parts of an industrial ecosystem that exist coherently enough with each other to make the whole worth more than the sum of its parts.[37] For the U.S. EW ecosystem, this includes a broad swath of commercial commodity suppliers, component manufacturers, subsystem developers, and system integrators as well as non-commercial entities (Figure 2) that directly support EW. It also includes related industries that tangentially support EW: cellular communications, autonomous cars, sensors, microelectronics, and unmanned systems. As Porter's study found, the biggest advantage of related and supporting industries comes from a closely knit web of relationships between organizations that communicate regularly, exchange ideas and innovations, and influence each other's R&D work.[38] Consequently, the most value for the U.S. EW ecosystem is when clusters of these organizations collaborate.

During visits with EW-related companies in spring 2023, individuals associated with commercial firms regularly spoke of cooperation and co-development with these related and supporting organizations. However, the largest firms frequently have more power than other organizations, which can have detrimental impacts on cooperation and innovation. For instance, if a very large firm decides that a certain design or process is better for their business model, then they may not objectively consider alternative design options put forward by a smaller collaboration partner. But as Porter pointed out, sometimes disadvantages create new opportunities for innovation and production.[39] Given favorable factor conditions elsewhere, such as targeted private or government investment, this power differential may force others in the U.S.

EW ecosystem to create new relationships or develop new technologies that will create a competitive differentiation advantage, such as finding new ways to integrate dual use technology into EW systems for the military.

Finally, the fourth attribute covers firm structure, strategy, and rivalry.[40] The structure of U.S. EW firms parallels that of other defense industries. At the top of a flat pyramid there is a loose oligopoly – a handful of very large "prime" companies with the resources to build complex defense systems and integrate subsystems into them. Next are the dozens of companies developing complete EW systems that can be integrated into those platforms. Then, there are hundreds of companies that develop subsystems, such as electronics modules and power management systems. The base of the pyramid is composed of the thousands of companies that provide components and commodities.[41]

Depending on the terms in the government's requests for proposals, companies (typically traditional prime companies) may use price or product differentiation strategies to compete with rivals for EW-related contracts. As part of their competition strategies, nontraditional companies are focused on making use of dual use technologies wherever possible to provide innovative EW solutions differentiated from the offerings of traditional companies.[42,43] For example, the DoD is widely adopting unmanned systems, which are far less complex than jets or ships.[44,45] Many unmanned aircraft systems are either modified COTS or GOTS products designed with modularity in mind. This design choice makes it easier to integrate a variety of payloads (i.e., EW solutions), which makes this an attractive area for nontraditional companies to use product differentiation strategies to compete with rivals, especially traditional prime companies, for EW-related contracts. However, both industry and the government need to consider the trade-offs involved in using commercial products to respond to DoD demand, including the fact that many EW requirements cannot be met by wholly COTS or even modified COTS products due to the uniquely military nature of EW systems. Commercial technology development in related areas certainly provides benefits for the EW ecosystem. But for operational EW systems themselves, dual use technologies appear to be most useful for prototyping and as labor-saving production equipment.

Industry Analysis Conclusion

As assessed through the lens of the Porter's Diamond model, this industry will likely continue to meet the military's current requirements for EW systems because the EW ecosystem derives positive benefits from:

- the commercial development of technologies tangential to EW,
- EW systems based on real-world experience and sold by partner nations' subsidiaries,
- the increasing use of open system architectures, which allows products from different manufacturers to function together,
- using COTS-based solutions for rapid prototyping,
- collaboration between clusters of EW-related organizations, and
- nontraditional firms using product differentiation competition strategies, which increases the variety of solutions being offered to the DoD.

On the other hand, the U.S. EW ecosystem's ability to develop innovative future solutions is sometimes limited by the government because the DoD does not communicate a clear demand signal about its future EW needs and the military services do not critically assess whether an 80 percent solution, such as a solution provided by COTS products, is enough to meet their needs. This last challenge is especially important because, due to the uniquely military nature of EW systems, COTS products are not always going to be sufficient in spite of the DoD's preferences.

The next two sections of this paper explore the ways in which the DoD has created impediments to industry innovation. These impediments include EW organizational challenges, government-wide barriers to collaboration, and the military's ability to absorb industry's EW innovations and effectively put them to operational use.

Impediments to EW Innovation

"World War II Army Gen. Montgomery had a very famous quote where he said, 'If we lose the war in the air, we'll lose the war and we'll lose it quickly'... And I would offer it today, this many years later, if we lose the war on the electromagnetic spectrum, we're going to lose the war and lose it quickly."[46]

– General Mark Kelly, Commander, U.S. Air Force Air Combat Command

The U.S. EW ecosystem derives positive benefits from the factors listed in the previous section, but it also faces roadblocks to innovation, such as a muddled demand signal and government decisions that decelerate the development of products in early technology readiness levels. This section addresses DoD organizational challenges and barriers, including the need for department and service level leadership with EW operational experience, increased use of data science within the DoD and IC, system architectures that share data freely, reduced classification barriers, and increased international and domestic cooperation. The DoD can and should take steps to remove impediments and roadblocks to EW innovation, collaboration, and technologies development across the EW ecosystem in support of U.S. EMS superiority.

Empowered and Centralized DoD EW Leadership

There are barriers created by the military services that impede EW innovation, prioritization, and integration within and amongst the DoD and services. Many of the barriers that hinder the optimization of EW capability stem from an overall deficit of operational EW experience, which is vital to understanding the ends, ways, and means to integrate EW effects. The U.S. Government Affairs Office (GAO) has executed multiple studies over the last decade, repeatedly identifying that the DoD's actions have not fully addressed a critical leadership gap for EMSO oversight. The GAO identified the leadership gap as "the highest priority, but also a prerequisite to addressing the other 33 gaps."[47] Leadership, strategy implementation, oversight processes, integration of EW technologies, and the modernization of the military services are other barriers the GAO identified for the DoD and services to meet national strategy requirements.[48] Service modernization is key to integrating advanced EW capabilities, yet that effort is faced with similar challenges. Without a central EW integrator and EW operationally experienced leaders striving for service modernization and joint interoperability, the DoD's EW demand signals to industry will be muddled, blurring industry's focus and stymying DoD's efforts to achieve the EMSO strategy goals in the 2020 EMSSS.

The 2023 Service Posture Reviews provided to Congressional defense committees show divergence in how the military service modernization plans prioritize EW capabilities. The Air Force intends to stay aligned with the Secretary of the Air Force's seven operational imperatives and views EW as a cross-cutting operational enabler, but the Air Force did not prioritize specific EW capabilities or systems, which leaves EW modernization to future budgets.[49] The Navy did not specifically reference EW but desires to posture around platforms that champion manned and unmanned capabilities, teaming those systems and capabilities.[50,51] The Marine Corps is aggressively modernizing its force while integrating EW systems and capabilities down to company levels across multiple devices and platforms.[52] The Army signaled that EW remains tied to the intelligence community (IC) and cyber but without specific actions or procurements.[53,54] This divergence amongst the services sends a confusing signal to Congress and the EW industry that impedes the holistic advancement of EW capability, creates duplication, and generates conflict at the point of integration. Furthermore, service priorities are influenced by an outdated DoD readiness reporting system (DRRS) that focuses more on availability for delivery rather than the effects of assigned tasks, such as EW.[55] Military service leaders should focus on achieving the 2020 EMSSS goals by pursuing total force EMS readiness through a process of continuous culture improvement, service modernization, and the incorporation of cutting-edge technologies supporting EW capabilities.

To change behavior and improve integration across the DoD's EMSO activities, the DoD should appoint a lead integrator across its EMS community. There is already a Director for EW position that falls within the Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)), but the authority of this position appears limited, and the title 'director' may be misleading. These claims are not judging the Director's leadership or integration efforts but reflect the DoD's failure to empower the position appropriately. The Director supports the Platforms and Weapons Portfolio Manager (P&WPM) in OUSD(A&S). The organizational hierarchy of this position lacks the authority, and therefore the opportunity, to fully integrate and prioritize EMSO across the entirety of the Office of the Secretary of Defense (OSD), including research and engineering, science and technology, and other core functions that influence EMSO. Without the authority to mandate or force stakeholder action, the 'director' role is limited. The position's authorities insufficiently provide the formal connective integration with the warfighter's requirements and strategic vision, including the Joint Staff's Joint Warfighting Concept (JWC). Additional authorities, with military service participation, can strengthen EW innovation, acquisition, and integration with the Office of the Under Secretary for Policy, (OUSD(P)), and the Office of Cost Assessment and Program Evaluation (CAPE).

To advance EW innovation, prioritization, and effects, the Director of EW requires complete authority and autonomy to direct (as the title alludes) and prioritize EMSO capabilities across the DoD. Authority should be used to assign a military service-aligned deputy director of EW to help drive integration. As most of the budget's total obligation authority lies within the DoD's services, an assigned service deputy director of EW would be best positioned to influence service integration and collaboration on the enterprise's requirements (in conjunction with organizing, training, and equipping the individual services) through policy and budgeting. Such a person could also focus on managing equitable contributions across OSD while injecting the warfighter's strategic vision and requirements pathway through the JWC. It is still valuable for the services to preserve service-unique EW capabilities, but centralized authority and coordination should increase collaboration, joint integration, and interoperability.

Recommendation #1: *Authorize the Director of EW (OUSD(A&S)) to establish a Joint EMSO Office led by a Military Flag Officer as Deputy Director of EW. Dissolve EMSO cross-functional teams (CFTs) and establish divisions under the Joint EMSO Office for spectrum and battle management, EW capability acquisition, and EW capability integration. The joint EMSO office would utilize equitable service-TOA to manage EW procurement via OUSD(A&S) and collaborate with OUSD(R&E) and the Joint Staff for integration and to address EMSO capability gaps.*

Data Science Applications for EW

The DoD and IC collect, process, and exploit more structured and unstructured data than ever before from private and public entities, including allied and liaison partners, foreign targets, and consumers. The increasingly large amount of data being collected makes it ever more difficult to transform that data into information, knowledge, and intelligence judgments. However, the challenge of having immense amounts of data also provides new opportunities.[56] According to Cathy Johnson, former Defense Intelligence Agency (DIA) Director for Analysis, "Hidden in this immense volume of data are new information, facts, relationships, indicators, and points that either could not be practically discovered in the past or simply did not exist before."[57] Data science is a multidisciplinary field that can help the DoD and IC manage data in new ways and to find those hidden connections that lead to better intelligence judgments.

Data science requires critical technologies and vast amounts of data. Neither the 2020 EMSSS nor the 2022 National Security Strategy (NSS) mention data science, but the EMSSS does discuss the use of technologies helpful to data science, such as AI and ML[58] while the NSS emphasizes the need to embrace new data analytic tools for enhanced decision making.[59] The EW mission presents an interesting area for the application of data science. The application of data science to EW is relatively new at the conceptual level, but the issues involved are not unique. The DoD and IC have been challenged for decades by extensive amounts of EW data and are further afflicted by a lack of data science, which is a problem that is exacerbated by a decline in trained manpower.

In spring 2023, a focus group of subject matter experts from the National Air and Space Intelligence Center (NASIC), Air Force Research Laboratories (AFRL), Naval Surface Warfare Center (NSWC), RAND Corporation, and Riverside Research explored the need for data science in EW. The focus group defined EW data science specifically as the use of a multidisciplinary approach, including mathematics, statistics, AI, computer science, applied physics, electrical engineering, and computer engineering, to analyze, process, and exploit data collected by a variety of sensors in order to extract meaningful insights.[60] The focus group identified core issues for EW data science. The issues that will be covered in this section are:

- data scientists are difficult to recruit and retain under current government pay structures,
- a lack of sufficiently labeled data caused by a lack of overall data standardization, and
- the use of an array of unique data management platforms and automation and analysis software applications.[61]

The personnel-related issues are critical. Most of the focus group participants reported that they have had data scientists intermittently involved in their teams, but they disappear too soon to make a long-term difference. This means that the amount of data analyzed by humans and automated tools is very low, and the amount of data not analyzed at all remains very high.[62] Data scientists need to have full-time roles on these teams, much like other disciplines. The DoD and IC have a few data scientist development programs, but there are still significant challenges recruiting and retaining people with this skill set. The DoD and IC need to adjust policies, establish development and hiring programs, offer incentives, and create data science centers of excellence. The dearth of data scientists needs to be managed in the short-term by sharing skills with data analysts until personnel investments show sustainable success.

The process issues are the most complex. Title 10 and Title 50 regulations make it extremely difficult for DoD and IC organizations to share data. Organizational stovepipes, regulatory requirements, and classification differences have led to the development of bespoke and disparate data management platforms. Organizations use different tagging, labeling, and formatting schemes, which makes it very difficult to share and analyze data. While it is technically feasible to develop common data management platforms, regulatory and compliance concerns make this concept difficult. However, if the relevant agencies were to collaborate to establish a common data management platform, EW sample data could be used for a pilot program or test case. The focus group also indicated that there are a multitude of different COTS and GOTS analysis and automation software applications throughout the DoD and IC, likely caused by decades of mission, compliance, and cultural differences. This decreases the ability of organizations to collaborate on automated analytical efforts. OUSD(A&S), OUSD(I&S), and the Defense Standardization Program need to need to create a short list of allowable software applications and establish standards for tagging, labeling, and formatting EW data to enable better interoperability and efficiency.

Data science is a multidisciplinary approach that, if applied consistently by the DoD and IC, could provide enormous benefits for collaboration and innovation both within the government and between government organizations and industry. Resolving data science issues would remove impediments to improving the analysis and usage of collected EW data.

Recommendation #2: *The DoD and IC must bolster data science hiring programs to address an overwhelming intelligence weakness. DoD and IC should consolidate analysis and automation software applications/platforms and standardize data formats to increase efficiency and effectiveness.*

Open System Architectures

Although some EW acquisition program offices in DoD have adopted open system architectures (OSA) and interoperability standards, others have not. Closed system designs lead to collaboration challenges, data that cannot move freely, and vendor lock. OSA is a system design that allows interconnectivity and compatibility between two or more dissimilar systems.[63] It is designed to integrate components of different types easily, enabling systems to stay updated with technological advances and increasing their longevity. Open architecture software and hardware provide immense opportunities for creating pre-configured software and hardware that can iteratively upgrade an EW system by swapping out components with minimal changes. Using OSA makes it easier for third-party developers, such as non-traditional and/or smaller defense companies, to extend the functionality of existing applications and systems and allows for a higher degree of innovation and flexibility. As different vendors contribute to an open EW architecture, government acquisition offices can integrate a more comprehensive range of capabilities into EW systems.

Better communication between EW users and developers allows both parties to voice their ideas early and often. When developers apply agile program management methods that emphasize an iterative and collaborative approach, they can incorporate operator feedback to adjust the design through multiple development cycles.[64] Agile software development methods are advantageous for open architecture applications because they allow developers to quickly adapt to changing requirements, enabling rapid EW product delivery.

During site visits to EW-related organizations in spring 2023, stakeholders identified closed system architectures as restricting the ability to detect threats, test systems, and update systems with the latest technology.[65] While a closed operating system architecture can protect against malicious activity by limiting attack pathways and preventing easy access to sensitive data, that is a trade-off with the resulting vendor lock, which tends to slow and reduce innovative system upgrades. Therefore, vendor lock can create a significant risk on the battlefield because the slow pace of upgrades mean that EW systems are relying on outdated technologies, which are less likely to detect or address emerging threats. Closed architectures also limit a system's ability to share data and interact with other systems, resulting in a lack of flexibility and scalability. These closed (i.e., proprietary) architectures limit troubleshooting to the original developer, ultimately ensuring a lock on continued system support, which drives up sustainment costs. One EW system developer, Mercury Systems, identified another primary cost driver: closed architectures can increase prices due to limited hardware and software supplies and customization capabilities.[66] Closed architectures can be more challenging to maintain due to a lack of access to bespoke system components.

Open system architectures coupled with standards for tagging, labeling, and formatting data can help align organizations' data interoperability, increase the speed at which data can be exchanged, and lead to faster decision-making. Closed systems and disparate data formats, in contrast, are roadblocks to an efficient EW ecosystem that collaborates and innovates. By instituting standards for EW data interoperability, EW systems can be compatible and capable of exchanging data securely and efficiently across organizations. This allows organizations to be sure their systems can work with third party hardware and software components, reducing confusion and providing assurance that data can be exchanged between systems.

Open system architecture approaches enable data-driven solutions to address EW wartime requirements. Open system architecture enables data and resources to be shared across multiple systems and allows for better integration and analysis of data collected from multiple sources, which will lead to new insights into adversarial threats and behaviors. If DoD acquisition program offices continue to move toward the use of OSA for EW systems, it will reduce costs by sharing components and resources between different systems and will reduce vendor lock by expanding development opportunities for third-party developers. Overall, OSA can increase collaboration within the government and industry, help data move more freely between organizations, and lead to more innovative EW capabilities that will ensure U.S. EMS superiority.

Recommendation #3: *The DoD must leverage open system architecture to ensure interoperability and compatibility among EW systems and critical data across multiple platforms and service components that are essential to national security.*

Classification of EW Programs and Information

The over-classification of EMS and EW programs, particularly into Special Access Programs (SAP) and sensitive compartmented intelligence (SCI), limits the ability of the EW industry to develop innovative technologies and solutions for DoD. Over-classification of EMS programs can impede collaboration, innovation, efficiency, and competition within the EW ecosystem, potentially limiting the effectiveness of these critical programs and undermining national security. The DoD must balance protecting classified information with fostering collaboration and innovation within the defense industry. When information about a program is classified, it is often difficult for EW firms and other stakeholders to understand requirements and objectives. This can impede collaboration between everyone involved and makes it challenging to develop innovative new technologies and solutions that meet DoD's needs.

The foundational document that governs classification is the 2009 Executive Order (EO) 13526, Classified National Security Information, which "prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism."[67] This EO details the different U.S.

government classification levels and describes the nature of harm of each should it be inappropriately disclosed. A key aspect of the EO directs that if there is significant doubt about an item's appropriate classification level, the default is that it shall be classified at the lower level.[68] EO 13526 also defines and explains that a SAP is a classification parameter that should be sparingly used when the "vulnerability or threat to particular information is exceptional, and the normal criteria for determining eligibility for access applicable to information classified at the same level are deemed insufficient to protect the information from unauthorized disclosure."[69] Only Principal and deputy-level government officials are authorized to establish SAPs, and the EO directs them to be kept to an absolute minimum based on necessity.[70] The ever-increasing number of DoD SAPs, specifically in the EW realm, suggests that the DoD is not adhering to the spirit of EO 13526.

Members of the EW ecosystem, including industry leaders, FFRDCs, and military organizations, indicated in spring 2023 that as EW systems are becoming more advanced, the trend is to make them more restricted in classification level. Many new EW platforms and capabilities are placed in SAPs and intelligence caveats, making it harder to execute and integrate across the enterprise.[71] While SAPs are applied to DoD programs to protect platforms and capabilities, SCI is managed by the IC with multiple additional caveats that can further limit access. The emerging multi-function capabilities with EW systems are now entangling SAPs and SCI, which complicates information sharing even more. Where once you only had a radar, a sensor, or a jamming capability, all the capabilities are now layered together in the same platform and integrated with real-time intelligence. The nexus of these new capabilities under SAP and SCI, particularly with electronic intelligence (ELINT), is a primary driver for the additional required classification. When asked about this trend, senior leaders at the Naval Air Warfare Center – Weapons Division (NAWC-WD) said the DoD is too conservative in classifying information, resulting in many stove-piped EW advancements causing multiple organizations to duplicate efforts because they lack awareness of parallel advancements. The desire to protect high-end technologies with SAPs and SCI is understandable. Still, it often comes at the cost of creating multiple silos of effort and further limiting expertise and available supporting infrastructure.[72] This point was driven home when a NAWC-WD senior engineer stated, "EW technology isn't the impediment anymore; it's our [DoD] systems and processes that are holding us back."[73]

Leaders within the DoD should relook at EO 13526 and evaluate the need for SAP programs in specific EW capabilities. A lower classification would open the capability to a broader workforce and more industry collaboration. There are likely SAPs that could have certain capabilities released from the SAP and classified at a lower lever level to broaden access. The DoD should also create more umbrella EMSO SAPs that cover specific capabilities instead of just a single platform. Umbrella SAPs allow for more collaboration, sharing, and testing across the EW enterprise. While umbrella SAPs and more liberal classifications may seem riskier up front for security reasons, the risk of inaction is an opportunity cost and may be ultimately riskier with respect to competition in the EMS. As Patrick Eddington and Christopher Preble said in a 2020 Defense360 article:

> The belief that limiting access to most information makes us safer is a fallacy; the opposite is probably closer to the truth. There will always be some risk that sensitive information will fall into the wrong hands. As it is today, however, there is an even greater risk that actionable intelligence will not fall into the right hands.[74]

***Recommendation #4:** DoD leaders should critically evaluate appropriate classification levels and seek to open information to a broader workforce, leading to more industry collaboration. When SAP classification is necessary, DoD leaders should encourage more use of umbrella SAPs to broaden collaboration, sharing, and testing across the EMSO enterprise.*

Domestic Collaboration and Innovation

One of the most common threads across multiple engagements with the EW ecosystem was the desire for more communication between DoD and the EW industry. SAPs and over-classification are key factors limiting industry EW innovation in line with the DoD's envisioned path forward. On the industry side, there is a push for more collaboration with DoD on future EW requirements so that industry can appropriately allocate their independent research and development (IR&D) dollars toward goals that will benefit them and the DoD.[75] An executive at L3 Harris said that it is hard to know what opportunities you can create when many technologies are hidden behind SAPs. He also requested that the DoD review the number of classified billets allocated to the EW industry. He claimed that more billets would expand the workforce of their R&D programs and provide the DoD with better offerings from industry.[76]

Another outcome of over-classification is that it can be difficult for small businesses and new entrants to the defense industry to compete with established players like the big defense prime companies, which have more access to classified information through existing contracts. This can limit innovation and competition within the industry, potentially leading to higher overall costs for the DoD. By providing clear guidance and requirements and investing in R&D, the DoD can promote better collaboration and innovation within the EW industry and help ensure the military services have access to the latest technologies needed for EMS superiority.

The DoD must create a culture that encourages more collaboration between the DoD and the EW industry. This can be achieved by establishing more robust partnerships and collaboration programs, providing incentives for nontraditional firms to collaborate with the DoD, and promoting open communication channels between military, industry, and academic experts. Specifically, the DoD could establish routinely held, OSD-chaired working groups that include joint and service-level EW leaders, academics and scientists, and industry leaders to share relevant information and break down barriers. As a result, all EW stakeholders would better understand each other's needs and capabilities and quickly identify further collaboration and innovation opportunities.

The DoD must also better articulate guidance and requirements to industry partners regarding what is required to meet current and future EW challenges. This could involve identifying capability gaps, prioritizing areas for development, and communicating mission requirements to industry partners. Innovation in the EW ecosystem would be better served by more descriptive requirements and reference missions from DoD, not prescriptive requirements with explicit specifications. This type of communication would help the EW industry with its IR&D investments. The Office of the Under Secretary of Defense for Research and Engineering, OUSD(R&E), should develop an EW Technology Roadmap and share that roadmap with industry to guide IR&D and other investments. OUSD(R&E) should assign stewardship of specific areas in the roadmap to the Defense Advanced Research Projects Agency (DARPA), Defense Innovation Unit (DIU), government labs, AFWerx, and other relevant organizations. When the EW industry is left guessing about how to invest its IR&D dollars, there is a good chance that EW R&D becomes a bill-payer for other technology areas or firms unknowingly invest in areas that the DoD is not interested in pursuing.[77]

Recommendation #5: *DoD must better articulate guidance and requirements to industry partners on what is required to meet current and future EW challenges. OUSD(R&E) should develop an EW Technology Roadmap, assign DARPA, DIU, labs, AFWerx, etc., as stewards of specific S&T and R&D areas, and share that roadmap with industry to guide IR&D and other investments.*

International Collaboration and Innovation

Slow and inefficient processes related to international collaboration are also impediments to innovation. This is true despite a national security posture rooted in strong alliances built over decades.[78] Key roadblocks include U.S. export control processes and domestic manufacturing laws and regulations that create barriers to entry into the U.S. defense ecosystem.

The United States has a robust export control infrastructure with the International Traffic in Arms Regulations (ITAR) for weapons and defense articles and the Export Administration Regulations (EAR) for dual-use commercial items with defense applications.[79] While the cognizant organizations involved in both processes do a good job, the processes require significant time to complete. At best the long timelines delay sales. At worst the long timelines deter firms from entering the defense technology markets entirely.

In 2020 alone, the Department of Commerce's Bureau of Industry and Security received over 39,000 requests for dual-use licenses – a volume that creates delay despite the best efforts of those involved.[80] Export regulations are based solely on the item being exported and not on the recipient nation. This is often followed by even more process in the form of waiver requests, even for the most trusted military allies of the United States.[81] While export controls perform a vital role, it makes little sense to continue to go through such a lengthy process for technical collaboration crucial to national defense with trusted, technologically adept military allies.

The United States should create a 'default to yes' approach and develop a short list of key defense technologies in which trusted military allies have demonstrated capability. The United States already has existing defense arrangements, especially with Canada, that provide a blueprint for increased engagement along these lines.[82] While creating and reviewing any such list would take time, the subsequent collaboration in that space would be spared the normal time-intensive process. Government reference architectures and technical baselines can also help define the boundaries of the allowable 'default to yes' spaces. Bilateral sharing is more politically palatable than simply sharing U.S. information unilaterally. While bilateral agreements leading to shared information will take time to build, they will increase collaboration opportunities, interoperability, and innovation with allies.

Within the United States, there are laws and regulations that make it difficult for foreign firms, even firms based in trusted allied countries, to do business. The Buy American Act, which was recently strengthened to increase government purchases from domestic sources, is a prominent example.[83] Major defense firms from trusted, militarily capable allies are interested in doing defense work in the United States. Subsidiaries of foreign defense firms must clear security requirements, security restrictions, and a review by the Committee on Foreign Investment in the United States.[84] The firms thus created provide jobs for American citizens, bring new technology to bear on critical U.S. defense areas like EW, and open a venue for collaboration and information sharing. Barriers to entry make even less sense given the pacing threat of China and the decrease in the U.S. defense ecosystem since the Cold War.[85]

The United States is stronger and more innovative in defense technology with trusted, technologically and militarily capable allies than without. Removing roadblocks to collaboration and impediments to innovation in EW should be a top priority for national leadership.

Recommendation #6: *The United States should expand current defense technology sharing efforts to create a 'default to yes' pre-approved short-list in ITAR and EAR. Trusted military allies with demonstrated capability in key defense technologies could be added to the list following approval by the Departments of State, Commerce, and Defense.*

EW Innovation Conclusion

This section evaluated impediments to innovation, organizational challenges, and barriers to collaboration in the areas of leadership, data science, open system architecture, classification, and domestic and international barriers. There is a clear need to remove roadblocks to collaboration within the EW ecosystem by implementing a DoD lead integration role, growing the data science workforce to address intelligence data management and analysis issues, and leveraging OSA for EW interoperability across platforms. Domestic barriers can be reduced by reevaluating the classification of SAP programs, utilizing SAP umbrellas, and better communicating requirements to industry to guide their R&D investments toward the DoD's EW needs. International barriers can be reduced by using proactive approaches to acquiring technology through trusted bilateral sharing and the creation of a 'default to yes' list for exports to militarily and technologically capable allies. Implementing these recommendations will improve collaboration and innovation and bolster U.S. efforts to maintain EMS superiority.

Moving From Innovation to Operational Effectiveness

"Providing EMS capabilities to the joint force is an absolute prerequisite for any deterrence or combat victory."[86]

– General Charles Q. Brown, U.S. Air Force Chief of Staff

While the impediments to EW innovation are significant, the barriers to translating maturing EW technologies and operational concepts into the military are likely even greater. Large bureaucracies are resistant to change, and the DoD is one of the largest bureaucracies in the world. Much of this resistance is unintentional and simply due to organizational inertia. For example, when someone is tasked with updating a doctrinal publication or a training plan, they start from the previous version and rarely with a clean sheet of paper. Many of these impediments to operational absorption can be overcome through collaboration, awareness, and the use of new technologies. This section of the paper examines key impediments to quickly translating new innovations into operational capabilities. A first foundational step toward increasing operational effectiveness in the EMS would be to make significant changes to key doctrinal Joint Publications. Next, the DoD should simultaneously make organizational changes and leverage new technologies to improve the spectrum management, training, and threat data sharing needed to translate EW technologies into operational advantage. Lastly, advances in EW innovation and technology will not matter if the DoD fails to effectively prepare for their use in a combat environment through innovations in EW training.

Joint EW Environment

EW is lacking a joint construct that will enable joint success. Despite the Joint Staff's efforts to update JP 1, the "capstone [JP],"[87] Joint Staff paradigms are failing to keep up with the evolution of the National Military Strategy and the last two National Defense Strategies. JP 1 does not consistently distinguish between cyber and EW. Chapter 1 of the draft publication defines the term “all-domain” to include the physical domains (land, maritime, air, and space) and the information environment, which includes cyberspace and, by default, EMS. Later in the text, it defines the operational environment as one that “encompasses the physical domains of air, land, maritime, and space; the information environment (which includes cyberspace); and the electromagnetic spectrum.” This latter definition indicates that the EMS is a separate domain distinct from the information and cyber domains, yet the Joint Staff seems to conflate the two. This conflation may appear to be of minor consequence, but it leads to elements in DoD inconsistently aligning the EMS portfolio under CIO, CTO, or cyber organizations. Clarifying DoD’s view on where EMSO fits is an essential first step.

Additionally, JP 5-0, the “keystone document for joint planning,”[88] refers to each domain throughout the document multiple times (see Figure 3). In contrast, there is only a single reference to EW, “electronicmagnetic[sic] warfare,” and it is mis-spelled. Despite being published just two months after the 2020 EMSSS, JP 5-0 failed to integrate the EMSSS’s strategic goals into this keystone document, leaving its users without a framework to effectively integrate the DoD’s EMS strategy into joint and service planning. Additionally, JP 3-85, “Joint Electromagnetic Spectrum Operations,” which is the publication charged with providing “fundamental principles and guidance for planning, executing, and assessing [JEMSO] across the competition continuum,”[89] hasn’t been updated since May 2020, demonstrating a lack of emphasis in fully integrating the EMS strategy across the joint force. This is a critical gap if the United States intends to dominate the EMS. The pace of the evolving operating environment and

Domain	**References in JP 5-0**
Cyberspace	33 references
Air	17 references
Land	14 references
Maritime	11 references
EW	1 reference

Figure 3: JP 5-0 Domain References

the associated changes in the character of future war requires more than multi-year reviews of simple changes to capstone or keystone documents.

The EMSSS provided enhanced understanding of DoD's approach to obtaining superiority, but it has not resulted in changes to doctrine at the service or the joint level, leaving the strategy interesting to those only with an interest in it. Integrating it into our capstone and keystone documents and professional military education programs will better prepare the force to face a future adversary in this domain and will guide efforts to link the development and employment of EW systems.

Recommendation #7: *DoD must establish where EMS fits in from a domain perspective; must integrate its application to tactics and operations down to the lowest echelon and across all domains using capstone and keystone joint doctrine; and integrate EMSO into Professional Military Education. Doing so will make EMSO ubiquitous, removing barriers that limit its understanding.*

Electromagnetic Spectrum Management

This portion of the paper focuses on the DoD's need for critical frequency bands within the EMS for spectrum-dependent communications and data transmittal. Numerous private and government organizations exist for the purpose of managing EMS deconfliction within national borders, regional sectors, and globally, providing designated frequency band users access while minimizing unintentional denials of service and signal interference. However, the EMS is growing more and more congested, making it challenging to manage and impacting the military's ability to operate in the EMS.

The Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) jointly manage the EMS to synchronize the interests of the U.S. government, the private sector, and the public within the airspace and borders of the United States.[90] The FCC, as an independent agency within the federal government, controls non-federal EMS usage by assigning or licensing frequency bands to nonfederal users. At the same time, the NTIA manages federal EMS usage by assigning frequency bands to federal agencies in the United States. As new spectrum-dependent technologies evolved over the last 50 years, the FCC and NTIA have used techniques, such as spectrum clearing, spectrum auctioning, and spectrum splicing, to maximize EMS availability and balance demands.[91]

The 2020 EMSSS highlights the integration of spectrum management and EW into what the DoD calls electromagnetic spectrum operations (EMSO).[92] This updated strategy recognizes the importance the spectrum plays in modern warfighting. The ability of friendly forces to utilize the spectrum and to deny the enemy that same spectrum creates a natural and required pairing of EMS management and EW. Specific spectrum-based command and control is needed to achieve EMS superiority, and electromagnetic battle management (EMBM) efforts aim to achieve this goal. EMBM is "a comprehensive framework for dynamic monitoring, assessing, planning, and directing of operations in the EMS in support of the commander's concept of operations."[93] Central to any successful EMBM system is the ability to conduct spectrum management.

External and internal challenges impact DoD EMS management and operations. A recent external challenge came to a head in April 2020, when the FCC unanimously approved Ligado Networks, LLC's application to deploy a terrestrial nationwide network operating in the same frequency bands with signals from satellites to GPS receivers.[94] The DoD and NTIA opposed the FCC's decision due to legitimate concerns for signal interference with GPS ground receivers. Following a congressionally mandated National Academies of Sciences, Engineering, and Medicine (NASEM) technical assessment confirming "harmful interference from their [Ligado's network] downlinks" with GPS and other mobile satellite receivers, the Senate Armed Services Committee asked the FCC to reconsider its Ligado approval.[95] In September 2022, Ligado officially paused its network deployment to resolve issues identified with GPS interference.[96]

Despite a reprieve for DoD on the potential Ligado interference, the House passed the Spectrum Innovation Act in July 2022, mandating the FCC to auction off the 3.1-3.45 GHz band while expecting DoD to vacate the S-band, which is the band primarily used by DoD for ground, air, and sea-based radars.[97] The Assistant Secretary of Defense for Space Policy, Dr. John Plumb, testified to a subcommittee of the House Armed Services Committee that the S-band "from 3.1 to 3.45 [GHz] is absolutely essential for DoD operations."[98] He further explained that to vacate the mid-band EMS for commercial 5G usage "would easily cost $120 billion, probably more, just to create the pieces, [and] could take easily 20 years" to develop the technology to replace the current Aegis Combat System.[99] As of April 2023, the DoD and NTIA succeeded in delaying FCC auctions until NTIA completed its study on spectrum band sharing between federal and non-federal entities, as directed in the Consolidated Appropriations Act of 2023. One possible solution for reducing future spectrum sharing issues is to for the FCC and NTIA to jointly mitigate and approve spectrum sharing requests.

Recommendation #8: *DoD should provide a legislative proposal requiring the FCC and NTIA to jointly mitigate interference and approve spectrum sharing between commercial and federal agencies while charging licensing fees for commercial usage of federal spectrum bands. Federal agencies invest revenue from commercial licensing fees toward R&D for improved spectrum sharing and relocation.*

There are two main internal challenges affecting DoD EMS management: organization systems and real-time EMS management. First, the number of organizations and systems the DoD uses for spectrum management is vast. A 2022 GAO report noted that multiple DoD entities are responsible for spectrum management and highlights how each military department has responsibilities and systems to accomplish spectrum management.[100] The report also listed 20 information technology (IT) systems the DoD uses for spectrum management and five Navy-specific tools.[101] Many organizations and 25 systems do not create streamlined joint spectrum management. Second, despite all of these spectrum management IT systems, the capabilities provided to an overall EMBM system are primarily in the planning rather than execution realm. An earlier 2020 GAO report noted that "a DoD official confirmed that the department does not use its predominant electromagnetic battle management system to adjust spectrum allocations in real time."[102] A critical component of EMBM is real-time decision support. The EMBM system of systems must be able to adjust frequency allocations in real-time to support complex EMSO to combat adversary spectrum operations or spectrum interference. A chaotic spectrum management environment and lack of real-time tools hamper current EMBM efforts.

Recommendation #9: *As part of a Joint EMSO Office (Recommendation #1), an EMBM division would enable efforts to develop robust EMS C2, including tools to support real-time spectrum management (e.g., JADC2). This division should focus on selecting a solution for EMBM and promulgating it across the Joint Force. This division would expand EMS C2 to all EW-related capabilities.*

Reality-Based EW Training

Just as the DoD's spectrum management processes require modernization, the advancement of EW system technology requires changes to experimentation and training for new EW capabilities to be effective. Without realistic training, even the most innovative new EW capabilities will not result in critical operational effects during times of conflict. The 2020 EMSSS states that the "training infrastructure must prepare the joint force to operate when freedom of action in the EMS is denied or contested."[103] Experimenting in a realistic EMOE is necessary to develop the operational concepts and tactics supported by the latest EW technologies. Training in a realistic environment ensures that all levels of operators are capable of effectively using EW systems. Although EW training is currently occurring, it is primarily conducted for small groups of personnel with little EW training taking place outside of the air and sea domains. In 2021, the DoD spent over nine billion dollars for the development and procurement of EW capabilities.[104] Those funds can only translate into operational effects if military operators know how to use them.

There are several security obstacles to realistic open-air experimentation and training. Developing EW simulators and training devices with updated Wartime Reserve Modes (WARMs) is one way of mitigating those obstacles. EW capabilities are proliferating throughout DoD systems, but there is a critical lack of training opportunities for operators throughout all levels of the military. Fortunately, this problem is solvable. The DoD solved a similar problem with flight training nearly a century ago when, in 1929, Edwin Link created the Link Flight Trainer that was used extensively for training World War II pilots.[105] The use of training devices to increase readiness can be expanded beyond the air domain and used to increase the entire DoD's ability to conduct effective EMSO. The same data and modeling capabilities that are needed for EW development, acquisition, testing and operations can also be used to create relatively low-cost EW training devices and simulators for operators across all domains of warfare. The 2020 EMSSS called for training to "be tailored to meet the needs of personnel at each level of Department structure – from technicians, to requirements personnel, to operators, and to top-level commanders."[106] Ubiquitous EW training capabilities – both open-air and simulated – are likely the only way this goal can be achieved.

Recommendation #10: *Each DoD service should incorporate simulator systems in conjunction with their EW system development. These simulators and training devices should be fielded for use across all echelons of the military and across all domains of warfare.*

Another challenge to realistic experimentation and training is the tension between using capabilities for training while safeguarding them from adversarial observation and exploitation. As the EMSSS pointed out, "the Department requires the ability to analyze and test EMS-dependent capabilities… while protecting classified information." This is challenging because, as much of America now appreciates thanks to a stray Chinese surveillance balloon, the military must assume that our electromagnetic emissions are constantly observed – even on and above our own soil. One technique that can mitigate the impact of this problem is by using WARMs. Joint Publication 3-85, Joint Electromagnetic Spectrum Operations, defines WARMs as "characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasure systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used but could be exploited or neutralized if known in advance."[107] WARMs are not a new concept, but they are more important now than ever and do not receive the attention they warrant. Systems with EW capabilities must include WARMs that are unique and rapidly updated based on known threats. Even though WARM information must remain protected, EW operators need to gain a foundational understanding of their application and an understanding of their effects on the EMOE. To achieve this, each EW system should include WARMs that are developed before system fielding, training should include the use of WARMs while not divulging the highly classified details, and the WARMs should be routinely updated as threats evolve. While simulated training and training for the use of WARMs can never achieve complete realism, with modern software and advanced EMS modeling, both can provide an essential component to improve overall EW training effectiveness.

Recommendation #11: *EW system acquisition offices must include requirements for a diverse suite of WARMs both during the development of the system and through routine software updates conducted throughout the life of the system.*

EWIR Process

The DoD's 2020 EMSSS calls for an "agile, fully integrated EMS infrastructure" that sustains all-domain advantage.[108] That infrastructure depends on the electronic warfare integrated reprogramming (EWIR) enterprise to compile, transfer, store, and exploit adversary threats by configuring friendly-force equipment for operational advantage.[109] The EWIR process is a key link between intelligence collection and EW operational effects, but with rare exceptions it is neither fast nor responsive. The process currently takes "at least several weeks, if not months to years."[110] Intelligence collection is not the problem. The DoD has adequate technology and sensors to collect large amounts of TECHELINT,[111] which is the branch of electronic intelligence that "describes the signal structure, emission characteristics, modes of operation, [and] emitter functions" of adversarial systems.[112] One of the major challenges to speeding up the EWIR process lies in the fact that TECHELINT is held within many disparate organizations within the DoD and IC. In addition to the data science approaches described earlier in this paper, economic theories provide a useful lens for framing and solving this problem.

Nobel prize winning economist James Buchanan studied a similar stove-piping phenomenon in commercial markets. Building on Paul Samuelson's Public Good Theory, Buchanan developed Club Good Theory. The key aspects of a club good are that it is excludable and non-rivalrous.[113] In a commercial setting, excludability prevents non-contributing members from gaining access to the benefits of membership, and non-rivalrous goods maintain their marginal benefit despite simultaneous usage. Figure 4 shows how club goods fit into the larger theoretical construct.

		Degree of exclusiveness	
		Excludable	Non-excludable
Degree of rivalry	Rivalrous	**Private goods:** food, clothing, cars, parking spaces **Private values:** For-profit; competition; reward; entitlement; innovation; scaling	**Common goods (common pool resources):** Fish stock, timber, coal, water, **Common values:** Common heritage; well-being; responsibility; collaboration; territorial integrity
	Non-rivalrous	**Club/social goods:** Cinemas, private parks, satellite television, ground **Club values:** Non-profit; belonging; trust; family, tribe; group interests; mutual support; community	**Public goods:** Television, air, national defense **Public values:** Non-profit; justice; safety; security; non-discrimination; public health; public interest

Source: Based on Crones, Sandler (1986); Van Tulder with Van der Zwart (2006)

Figure 4: Exclusiveness and Rivalry in Public Goods

Treating TECHELINT as a club good instead of a semi-private good, as it is currently treated, would reduce roadblocks in the EWIR process, helping it to move at an operationally relevant pace. Today, data exclusivity fractures ‘club membership’ into many isolated clubs, which fosters unproductive rivalry since EWIR stakeholders have limited access to TECHELINT outside their stove-piped intelligence agencies, military services, platforms, or programs. Data exclusivity manifests as SAPs, Special Technical Operations, service-centric relationships, and other silos. This results in incomplete threat awareness, poor modeling, and duplicative efforts within the EW ecosystem. Rivalry over the data increases as siloed groups differentiate their organizations to compete for R&D funding. Yet there is little reason to treat government owned TECHELINT as a rivalrous good across the DoD and IC. Certain aspects of data, such as sources and methods of collection, must be protected separately, but the primary data required for EWIR should be a club good shared across the enterprise.

As discussed earlier, data science is capable of processing and exploiting large amounts of EMS data. The first step to enable agile EWIR is to select and provide the necessary resources to a centralized data manager. NASIC is creating a common Electronic Attack Knowledge Base (EAKB). The effort is currently underfunded and is not designed to support all government consumers of TECHELINT, but those problems could be managed by treating EW data as a club good. The DoD could task NASIC with designing and managing the EAKB to provide common access to emitter raw I/Q data, mid-tier pulse level information (e.g., pulse descriptor word), and top-level metadata for the environment. Vetted EWIR stakeholders, including industry partners, could use the data for research, development, test, engineering, modeling, and awareness. Alternatively, to ease concerns about parochialism, the DoD could task DIA, which has signal intelligence oversight, or OUSD(I&S) with managing the EAKB.

Elevating the EAKB would enable a structure where government stakeholders provide funding to be part of the ‘club.’ The centralized data manager could receive a fee for each transaction or a pre-negotiated annual amount for providing the data infrastructure. This arrangement is not unusual in the DoD. For example, the Defense Logistics Agency receives funding from other DoD entities to procure, stock, and deliver equipment for maintenance and operations. Most national training and test ranges operate on a pay-to-play basis. In still other cases, acquisition offices and laboratories receive funding from other government entities to achieve efficiency in procurement. Creating a central TECHELINT data source would transform the current landscape from many information silos to a single, large source of information that would provide value to the myriad government and non-government EW stakeholders.

The DoD must translate intelligence into operational effects faster than adversaries can change their threats. The first step to accelerate the EWIR process is to treat EW data as a club good by creating a central repository that is accessible to an exclusive group of EWIR stakeholders. EWIR innovation is an internal roadblock the DoD can remove with funding and centralized management of a club good. The cost to do so is minimal compared to the cost in lives and equipment that will be lost in a conflict without U.S. EMS superiority.

Recommendation #12: *The DoD should establish a central data mechanism and manager for TECHELINT collaboration to reduce stove-piping and human-intensive processing across the EWIR enterprise. The data manager would receive funding from government organizations in exchange for access to the data needed to support the EWIR process across the EW enterprise.*

Operational Effectiveness Conclusion

Increasing leadership, advocacy, and the rate of innovation for EW capabilities will not contribute to combat effectiveness if the operational forces are not prepared to use those capabilities effectively. This begins with having clear doctrine related to EW that relieves the ambiguity about where EW fits in with respect to the current warfare domains and the concept of information operations. The DoD must also break down barriers to cooperating to achieve efficient spectrum management and to improve the use of valuable EWIR threat data. Finally, the

DoD must integrate EW training across the entirety of the force in a realistic environment to increase operational effectiveness.

Conclusion

Recent investments to drastically increase the production capacity of traditional munitions[114] are welcome and necessary to prepare for potential future conflicts. But with some estimates indicating that the DoD would run out of certain munitions in as little as one week in a theoretical conflict with China,[115] increasing munition production is far from sufficient to achieve deterrence or victory. The DoD dedicates funding to EW development, but there are many impediments to using those resources to create timely, innovative EW capabilities and to effectively transition those capabilities into the operational forces. The DoD must remove roadblocks to communication and collaboration within the DoD itself and throughout the broader EW ecosystem because restrictions on communication limit collaboration, which in turn hampers creativity and delays both EW-specific innovation and advances in related technology areas. Empowered EW leadership, multidisciplinary approaches to intelligence analysis, open system architectures, fewer classification barriers, clearer guidance to industry, and more open international relationships with allies are all actions the DoD can take to remove impediments to EW innovation. To make EW systems operationally effective, the DoD must fully integrate EW into joint doctrine, work with organizations external to DoD to maintain spectrum access, develop internal systems to conduct real-time EMBM, find ways to train all levels of operators on EW systems and effects, and improve the EWIR process. The DoD must make and guide investments to develop advanced EW capabilities and take bold actions to ensure those capabilities are operationally effective in combat if the United States intends to secure peace and maintain its global leadership status. The goals as stated in the 2020 EMSSS already point the DoD in the right direction. It is now a matter of executing the changes necessary to achieve those goals and the EMSSS's vision of U.S. EMS superiority.

1. Congressional Research Service, “FY2022 Electronic Warfare Funding Trends,” September 16, 2021, 1.

2. P.W. Singer and August Cole, *Ghost Fleet* (New York: Houghton Mifflin Harcourt, 2015).

3. Marine Corps War College, “Academic Year 2022 Reading List,” April 20, 2021, https://www.usmcu.edu/Portals/218/AY%2022%20Reading%20List_%20ver%2027%20Apr%2021.docx.

4. Department of Defense, “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2018,” May 16, 2018, 74.

5. Alex Marquardt, Natasha Bertrand, and Zachary Cohen, “Russia’s jamming of US-provided rocket systems complicates Ukraine’s war effort,” May 6, 2023, https://www.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html.

6. Helene Cooper, “ Biden to Name Air Force Chief to Top Military Post, Officials Say,” *New York Times*, May 4, 2023, https://www.nytimes.com/2023/05/04/us/politics/joint-chiefs-chairman-charles-q-brown-milley.html.

7. John A. Tirpak, “Brown: USAF Has Been ‘Asleep at the Wheel’ Too Long When It Comes to EMS,” *Association of Old Crows*, January 27, 2021, https://www.crows.org/news/549515/Brown-USAF-Has-Been-Asleep-at-the-Wheel-Too-Long-When-It-Comes-to-EMS.htm.

8. ”Joint Publication 3-85, Joint Electromagnetic Spectrum Operations,” May 22, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

9. Joint Publication 3-85, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

10. Courtney Kube and Mosheh Gains, “Air Force general predicts war with China in 2025, tells officers to prep by firing 'a clip' at a target, and 'aim for the head',” *NBC News*, January 27, 2023, https://www.nbcnews.com/politics/national-security/us-air-force-general-predicts-war-china-2025-memo-rcna67967.

11. Mallory Shelbourne, “Davidson: China Could Try to Take Control of Taiwan In ‘Next Six Years’,” *USNI News*, March 9, 2021, https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

12. U.S. Department of Defense, 2022a. National Defense Strategy (Washington, DC: Pentagon), 4.

13. U.S. Department of Defense, 2022a. National Defense Strategy (Washington, DC: Pentagon), 15.

14. U.S. Department of Defense, Electromagnetic Spectrum Superiority Strategy (Washington, DC: Pentagon), 1.

15. U.S. Department of Defense, 2022a. National Defense Strategy (Washington, DC: Pentagon), 4.

16. Graham Allison, Kevin Klyman, Karina Barbesino, and Hugo Yen, “The Great Tech Rivalry: China vs the U.S.,” Harvard Kennedy School’s Belfer Center for Science and International Affairs, December 2021, 2.

17. Graham Allison, Kevin Klyman, Karina Barbesino, and Hugo Yen, “The Great Tech Rivalry: China vs the U.S.,” Harvard Kennedy School’s Belfer Center for Science and International Affairs, December 2021, 4.

18. Michael Porter, “The Competitive Advantage of Nations.” Harvard Business Review, Volume 68, Issue 2, March/April 1990, 77.

19. U.S. Department of Defense, 1995, 2.

20. U.S. Department of Defense, 2020a, I-7.

21. John Rhea, “The Dilemma of Using COTS in Electronic Warfare Systems.” Military & Aerospace Electronics, September 1996, Vol 7, Issue 9. Accessed via EBSCO Host.

22. Porter, 77.

23. Porter, 78.

24. Steve Blank, "The Secret History of Silicon Valley," YouTube video, 1:02:46, posted by Computer History Museum, November 20, 2008. Accessed at https://www.youtube.com/watch?v=ZTC_RxWN_xo.

25. Gerald Stiles, "The Wild Weasel Development Programs." P-7661-RGS, July 1990 (Santa Monica, CA: The RAND Graduate School), 1.

26. DoD, Electromagnetic Spectrum Superiority Strategy, 5.

27. Porter, 77.

28. Secretary of Defense, "Specifications & Standards – A New Way of Doing Business." (Washington, DC: Pentagon), 1. Cited in "The Impact of Acquisition Reform on Department of Defense Specifications and Standards for Materials and Processes: Report of the Workshop on Technical Strategies for Adoption of Commercial Materials and Processing Standards in Defense Procurement," Appendix A "Perry Memorandum." National Academies Press. https://doi.org/10.17226/10345.

29. Rhea.

30. Rhea.

31. Rhea.

32. John McHale, "Obsolescence: Every COTS Designers Bad Dream." Military & Aerospace Electronics, February 1, 2000. Accessed at https://www.militaryaerospace.com/computers/article/16706594/obsolescence-every-cots-designers-bad-dream.

33. U.S. Department of Defense, 2020b, 9.

34. Kevin Morris, "Going Beyond COTS Strengthens Mil/Aero PLD Applications." Electronic Engineering Journal, May 30, 2006. Accessed at https://www.eejournal.com/article/20060530_altera/.

35. United States Air Force Scientific Advisory Board, Report on Ensuring Successful Implementation of Commercial Items in Air Force Systems. SAB-TR-99-03, April 2000. (Washington, DC: Pentagon), 26.

36. United States Air Force Scientific Advisory Board, 1.

37. Porter, 77.

38. Porter, 80.

39. Porter, 78.

40. Porter, 77.

41. U.S. Department of Defense, 2022b, 5.

42. Anduril, "Our Mission" website. Accessed April 29, 2023 at https://www.anduril.com/.

43. Epirus, "About Epirus" website. Accessed April 29, 2023 at https://www.epirusinc.com/about-epirus.

44. Joseph Trevithick, " 'Affordable Mass' Concept Driving Air Force's New Advanced Drone Initiative." The War Zone, March 10, 2023. Accessed at https://www.thedrive.com/the-war-zone/affordable-mass-concept-driving-air-forces-new-advanced-drone-initiative

45. Joseph Trevithick, "Navy Carrier-Based Drones Will Be Able to Be Controlled by the Air Force." The War Zone, April 5, 2023. https://www.thedrive.com/the-war-zone/navy-carrier-based-drones-will-be-able-to-be-controlled-by-the-air-force

46. Joseph Trevithick, "F-35 Patrols Near Russia Highlight Case For Cognitive Electronic Warfare," The Drive, April 28, 2023, https://www.thedrive.com/the-war-zone/f-35-patrols-near-russia-highlight-case-for-cognitive-electronic-warfare.

47. "Electronic Warfare, DOD Action Needed to Strengthen Management and Oversight," Report to the Committee on Armed Services, House of Representatives (Government Accountability Office, July 2012).

48. "Electromagnetic Spectrum Operations, DOD Needs to Take Action to Help Ensure Superiority" (Government Accountability Office, March 19, 2021).

49. "Department of the Air Force Posture Statement, Fiscal Year 2024, Department of the Air Force Presentation to the Committees and Subcommittees of the United States Senate and the House of Representatives 1st Session, 118th Congress," January 3, 2023.

50. “Statement of The Honorable Carlos Del Toro Secretary of the Navy, On Department of the Navy Posture, Before the Senate Committee on Appropriations” (Senate Committee on Appropriations, March 28, 2023).

51. “Statement of Admiral Michael M. Gilday Chief of Naval Operations, On the Posture of the United States Navy, Before the Senate Appropriations Committee” (Senate Committee on Appropriations, March 28, 2023).

52. “Statement of General David H. Berger, Commandant of the Marine Corps, On the Posture of The United States Marine Corps, Before the Senate Appropriations Committee” (Senate Committee on Appropriations, March 28, 2023).

53. “Statement By The Honorable Christine E. Wormuth Secretary of the Army, and General James C. McConville United States Army before the Committee on Armed Services United States Senate, 1st Session, 118th Congress, On the Posture of the United States Army” (Committee on Armed Services United States Senate, March 30, 2023).

54. “Statement by The Honorable Douglas R. Bush Assistant Secretary of the Army for Acquisition, Logistics and Technology and Army Acquisition Executive, and General James E. Rainey Commanding General Army Futures Command, and Major General Michelle A. Schmidt Director Force Development Deputy Chief of Staff of the Army G-8, Before the Subcommittee on Airland Committee on Armed Services United States Senate, On the Fiscal Year 2024 Army Modernization Program” (Subcommittee on Airland Committee on Armed Services United States Senate, April 18, 2023).

55. Bryan Clark, Dan Patt, and Timothy Walton, “Can the U.S. Regain Battlefield Superiority against China? Applying New Metrics to Build an Adaptable and Resilient Military,” Hudson Institute, January 2022, https://www.hudson.org/national-security-defense/can-the-u-s-regain-battlefield-superiority-against-china-applying-new-metrics-to-build-an-adaptable-and-resilient-military.

56. Bradley M. Knopp et al., “Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency” (RAND Corporation, November 18, 2016), https://www.rand.org/pubs/research_reports/RR1582.html. Ix.

57. Knopp et al. 1.

58. DoD, Electromagnetic Spectrum Superiority Strategy, 1-20.

59. “2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.Pdf,” accessed March 16, 2023, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF. 46.

60. An Exploratory Inquiry of Data Science in Electromagnetic Warfare Focus Group.

61. An Exploratory Inquiry of Data Science in Electromagnetic Warfare Focus Group., Google Drive, April 20, 2023.

62. An Exploratory Inquiry of Data Science in Electromagnetic Warfare Focus Group.

63. “Open-Standard System Architecture.” AcqNotes, August 6, 2021. https://acqnotes.com/acqnote/careerfields/open-standard-system-architecture.

64. “Agile | Software Engineering Institute.” Accessed April 25, 2023. https://www.sei.cmu.edu/our-work/agile/.

65. NDU Eisenhower School Electromagnetic Warfare Industry Study 2023.

66. Mercury Systems Site Visit Hudson, NH March 2nd, 2023, NDU Eisenhower School Electromagnetic Warfare Industry Study, Mercury Systems POC: Scott Derushia Scott.Derushia@mrcy.com.

67. Exec. Order No. 13526, § 4.3 (2009), https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information.

68. Exec. Order No. 13526.

69. Exec. Order No. 13526.

70. Exec. Order No. 13526.

71. Electromagnetic Warfare Industry Study Engagement Discussion, MAR-APR 2023.

72. Electromagnetic Warfare Industry Study Engagement Discussion, Navy Air Warfare Center – Weapons Division. APR 2023.

73. Electromagnetic Warfare Industry Study Engagement Discussion, Navy Air Warfare Center – Weapons Division. APR 2023.

74. Eddington, Patrick G, and Christopher A Preble. "Bad Idea: Overclassification." Defense360, December 1, 2020. https://defense360.csis.org/bad-idea-overclassification/.

75. Electromagnetic Warfare Industry Study Engagement Discussion, MAR-APR 2023.

76. Electromagnetic Warfare Industry Study Engagement Discussion, L3 Harris. APR 2023.

77. Electromagnetic Warfare Industry Study Engagement Discussion, MAR-APR 2023.

78. Biden-Harris Administration's National Security Strategy, The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (Accessed: April 29, 2023).

79. "Export Licensing - ITAR & EAR." Bureau of Industry Security. Accessed May 5, 2023. https://www.bis.doc.gov/index.php/documents/technology-evaluation/781-export-licensing/file.

80. "Statistics of 2020 BIS License Authorization." Bureau of Industry Security. Accessed April 30, 2023. https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/licensing-analysis/2841-statistics-of-2020-bis-licensing/file.

81. IS industry engagement discussion, 26 April 2023.

82. Hunter, Andrew P., Obecny, Kristina, & Sanders, Gregory, "U.S. - Canadian Defense Industrial Cooperation," Center for Strategic & International Studies, June 2017, U.S.-Canadian Defense Industrial Cooperation (csis-website-prod.s3.amazonaws.com), (Accessed May 12, 2023).

83. "The Biden Buy American Act: Changes That Significantly up the Ante." Venable LLP. Accessed April 29, 2023. https://www.venable.com/insights/publications/2021/08/the-biden-buy-american-act#:~:text=On%20July%2030%2C%202021%2C%20the%20Department%20of%20Defense,increasing%20transparency%20and%20accountability%20in%20Buy%20American%20rules.

84. Erwin, Sandra I. "Defense Contractor 'Reinvents Itself' to Operate Under Foreign Ownership." National Defense Magazine, May 12, 2015. https://www.nationaldefensemagazine.org/articles/2015/5/12/defense-contractor-reinvents-itself-to-operate-under-foreign-ownership.

85. Congressional Research Service, "Defense Primer: U.S. Defense Industrial Base," 17 April 2023, https://crsreports.congress.gov/product/pdf/IF/IF10548#:~:text=According%20to%20a%202022%20DOD%20report%2C%20the%20number,capacity%2C%20limiting%20competition%2C%20and%20undermining%20supply%20chain%20resilience (Accessed May 10, 2023).

86. John Tirpak, "Brown: USAF Has Been 'Asleep at the Wheel' Too Long When It Comes to EMS," Air & Space Forces Magazine (blog), January 28, 2021, https://www.airandspaceforces.com/brown-usaf-has-been-asleep-at-the-wheel-too-long-when-it-comes-to-ems/.

87. "Joint Publication 1, Volume 1: Joint Warfighting, Reference Copy," accessed April 28, 2023, https://jdeis.js.mil/jdeis/new_pubs/jp1_vol1.pdf.

88. "Joint Publication 5-0, Joint Planning," December 1, 2020, https://jdeis.js.mil/jdeis/new_pubs/jp5_0.pdf.

89. "Joint Publication 3-85, Joint Electromagnetic Spectrum Operations," May 22, 2020, https://jdeis.js.mil/jdeis/new_pubs/jp3_85.pdf.

90. John R. Hoehn, Jill C. Gallagher, and Kelley M. Sayler, "Overview of the Department of Defense Use of the Electromagnetic Spectrum," Congressional Research Service, R46564, (2021), https://crsreports.congress.gov/product/pdf/R/R46564.

91. Joseph Mitola III, Joseph Guerci, Jeff Reed, Yu-Dong Yao, Yingying Chen, T. Charles Clancy, Joahnna Dwyer, Hongbin Li, Hon Man, Robert McGwier, and Yi Guo, "Accelerating 5G QoE via Public-Private Spectrum Sharing, IEEE Communications Magazine, vol. 52, no. 5, 77-85, May 2014, https://ieeexplore.ieee.org/abstract/document/6815896.

92. Department of Defense, Electromagnetic Spectrum Superiority Strategy, 2.
93. Department of Defense, Electromagnetic Spectrum Superiority Strategy, 9.
94. Kelley M. Sayler and John R. Hoehn, "Implications of the FCC-Approved Ligado Network for the Department of Defense, Congressional Research Service, IN12028, (2022), https://crsreports.congress.gov/product/pdf/IN/IN12028/3.
95. Kelley M. Sayler and John R. Hoehn, https://crsreports.congress.gov/product/pdf/IN/IN12028/3.
96. Kelley M. Sayler and John R. Hoehn, https://crsreports.congress.gov/product/pdf/IN/IN12028/3.
97. Theresa Hitchens, "STRATCOM Wrapping Spectrum OPS Center Plan, as Military Faces Bandwidth Grab by 5G Firms," Breaking Defense, March 9, 2023, https://breakingdefense.com/2023/03/stratcom-wrapping-spectrum-ops-center-plan-as-military-faces-bandwidth-grab-by-5g-firms/.
98. Theresa Hitchens, https://breakingdefense.com/2023/03/stratcom-wrapping-spectrum-ops-center-plan-as-military-faces-bandwidth-grab-by-5g-firms/.
99. Jason Sherman, "Vacating Mid-band for Commercial 5G Would Cost DoD At Least $120 Billion and Take 20 Years," Inside Defense, March 9, 2023, https://insidedefense.com/daily-news/vacating-mid-band-commercial-5g-would-cost-dod-least-120-billion-and-take-20-years.
100. U.S. GAO, Spectrum Management: Information Technologies for Managing Federal Use, GAO-22-105221 (Washington, DC: Government Accountability Office, 2020), 12, https://www.gao.gov/assets/gao-22-105221.pdf.
101. U.S. GAO, Spectrum Management: Information Technologies for Managing Federal Use, 12, 13.
102. Joseph W. Kirschbaum, *Electromagnetic Spectrum Operations: DoD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64 (Washington, DC: Government Accountability Office, 2020), 24, https://www.gao.gov/products/gao-21-64.
103. DoD, Electromagnetic Spectrum Superiority Strategy, 13.
104. Congressional Research Service, "FY2022 Electronic Warfare Funding Trends," by John R. Hoehn, September 16, 2021, 2.
105. Naval Air Station Fort Lauderdale Museum, "The Link Training Flight Simulator," accessed on April 25, 2023, https://www.nasflmuseum.com/link-trainer.html.
106. DoD, Electromagnetic Spectrum Superiority Strategy, 13.
107. Department of Defense, "Joint Electromagnetic Spectrum Operations," JP 3-85, J7 Joint Force Development Directorate, 22 May 2020, 1-8.
108. DoD, Electromagnetic Spectrum Superiority Strategy, 5.
109. "Outsmarting Agile Adversaries in the Electromagnetic Spectrum" (Santa Monica, CA: RAND Corporation, 2023), v, https://doi.org/10.7249/RRA981-1.
110. "Outsmarting Agile Adversaries in the Electromagnetic Spectrum," 5.
111. Cognitive Electronic Warfare: Using AI to Solve EW Problems (USC Information Sciences Institute, 2023), https://www.youtube.com/watch?v=oO6piqNroiI; "Outsmarting Agile Adversaries in the Electromagnetic Spectrum," 80–92.
112. Richard L. Bernard, "Electronic Intelligence (ELINT) at NSA," Center for Cryptologic History, National Security Agency, 2009, 1.
113. James M. Buchanan, "An Economic Theory of Clubs," Economica 32, no. 125 (1965): 3, https://doi.org/10.2307/2552442.
114. Sam Skove, "US to Sextuple 155mm Production, Improve Arms Factories," Defense One, March 28, 2023, https://www.defenseone.com/policy/2023/03/us-sextuple-155mm-artillery-shell-production-replenish-stocks-sent-ukraine/384542/.
115. Seth G. Jones, "Empty Bins in a Wartime Environment," CSIS, January 2023, 1.

Appendix 1: Seminar Members and Faculty

Seminar Members:

Mr. William T. Althoff, Department of the Air Force

LTC Nancy E. Clauss, U.S. Army

LtCol Andrew D. D'Ambrogi, U.S. Marine Corps

LtCol Jayson M. Davidson, U.S. Marine Corps

Lt Col Kevin L. Jensen, U.S. Air Force

Dr. Quinn E. Lanzendorfer, National Security Agency

LTC Ryan M. Nacin, U.S. Army

Ms. Kathryn D. Parks, Department of the Air Force

Mr. Nicholas D. Pierce, Department of the Navy

LTC Ryan J. Pursel, U.S. Army

Mr. Robert J. Schadey, Department of the Army

Lt Col Scott M. Thompson, U.S. Air Force

Seminar Faculty:

Col Travis Ruhl, U.S. Air Force, Electromagnetic Warfare Study Lead

Mr. Luis Perez, DIA Chair and Assistant Professor

Appendix 2: Electromagnetic Warfare Visits and Lectures

<u>Government</u>

Air Force Research Laboratories
Defense Advanced Research Projects Agency (DARPA)
Director for Applied Technology (Office of the DCTO for Critical Technology), OUSD(R&E)
Director for Electronic Warfare and Acquisition, Integration and Interoperability Office, OUSD(A&S)
National Air and Space Intelligence Center
Naval Air Warfare Center – Weapons Division
Naval Research Laboratories
PEO, Intelligence, Electronic Warfare and Sensors (IEW&S), Army
Principal Director for Microelectronics, OUSD(R&E)

<u>Academia, FFRDCs, and Non-Profit Organizations</u>

Electronic System Design Alliance, SEMI
Massachusetts Institute of Technology Lincoln Labs
MITRE Corporation
RAND Corporation, Project Air Force
SRC, Inc.
University of Dayton Research Institute
Wright Brothers Institute

<u>Industry</u>

Amazon Web Services
Anduril
BAE Systems
Elbit Systems
Epirus, Inc.
HawkEye 360
Israel Aerospace Industries – ELTA Systems
L3Harris
Lockheed Martin Corporation
Mercury Systems
Northrop Grumman
Rafael Advanced Defense Systems
Raytheon Technologies
Sandbox AQ

Appendix 3: Summary of Recommendations

Recommendation	Estimated Resources Required	Proposed Office of Primary Responsibility (OPR)
Recommendation for Congressional Approval		
DoD should provide a legislative proposal requiring the FCC and NTIA to jointly mitigate EMS interference and approve spectrum sharing between commercial and federal agencies while charging licensing fees for commercial usage of federal spectrum bands. Federal agencies invest revenue from commercial licensing fees toward R&D for improved spectrum sharing and relocation.	**Est. Funding**: N/A **Est. Personnel**: Existing personnel	Assistant Secretary of Defense for Legislative Affairs, OSD(LA)
Interagency Recommendation for the Secretaries of State / Commerce / Defense		
The United States should expand current defense technology sharing efforts to create a 'default to yes' pre-approved short-list in ITAR and EAR. Trusted military allies with demonstrated capability in key defense technologies could be added to the list following approval by the Departments of State, Commerce, and Defense.	**Est. Funding**: N/A **Est. Personnel**: Existing personnel **Other**: While getting the pre-approvals set up will take staff time, subsequent efforts will save more time than the up-front efforts	Department of State; Department of Commerce; DoD
Interagency Recommendation for Department of Defense and Intelligence Community		
The DoD and IC must bolster data science hiring programs to address an overwhelming intelligence weakness. DoD and IC should consolidate analysis and automation software applications/platforms and standardize data formats to increase efficiency and effectiveness.	**Est. Funding**: $200M across FYDP to establish DoD-wide data scientist development programs **Est. Personnel**: Funding for new data scientist billets, if needed	Defense Civilian Personnel Advisory Services Defense Standardization Program OUSD(I&S)

Recommendation for Joint Staff		
DoD must establish where EMS fits in from a domain perspective; must integrate its application to tactics and operations down to the lowest echelon and across all domains using capstone and keystone joint doctrine; and integrate EMSO into Professional Military Education. Doing so will make EMSO ubiquitous, removing barriers that limit its understanding	**Est. Funding**: N/A **Est. Personnel**: Existing personnel **Other**: Modification to update timelines to enable updates to JP 1, JP 3-0, JP 3-85, and JP 5-0	J-7, Joint Staff
Recommendation for the Office of the Secretary of Defense		
DoD leaders should critically evaluate appropriate classification levels and seek to open information to a broader workforce, leading to more industry collaboration. When SAP classification is necessary, DoD leaders should encourage more use of umbrella SAPs to broaden collaboration, sharing, and testing across the EMSO enterprise.	**Est. Funding**: N/A **Est. Personnel**: Existing personnel **Other**: Leadership and advocacy; refresher training	DoD leadership, SAPCOs, and security managers at all levels
Recommendation for the Office of the Under Secretary of Defense, Research and Engineering		
DoD must better articulate guidance and requirements to industry partners on what is required to meet current and future EW challenges. OUSD(R&E) should develop an EW Technology Roadmap, assign DARPA, DIU, labs, AFWerx, etc., as stewards of specific S&T and R&D areas, and share that roadmap with industry to guide IR&D and other investments.	**Est. Funding**: Leverage existing RDT&E funding **Est. Personnel**: Existing personnel	OUSD(R&E)
Recommendation for the Office of the Under Secretary of Defense, Intelligence and Security		
The DoD should establish a central data mechanism and manager for TECHELINT collaboration to reduce stove-piping and human-intensive processing across the EWIR enterprise. The data manager would receive funding from government organizations in exchange for access to the data needed to support the EWIR process across the EW enterprise.	**Est. Funding:** Development cost estimate required **Est. Personnel:** Program office	OUSD(I&S) Alternative OPRs: NASIC or DIA

Recommendations for the Office of the Under Secretary of Defense, Acquisition and Sustainment		
Authorize the Director of EW (OUSD(A&S)) to establish a Joint EMSO Office led by a Military Flag Officer as Deputy Director of EW. Dissolve EMSO CFTs and establish divisions under the Joint EMSO Office for spectrum and battle management, EW capability acquisition, and EW capability integration. The joint EMSO office would utilize equitable service-TOA to manage EW procurement via OUSD(A&S) and collaborate with OUSD(R&E) and the Joint Staff for integration and to address EMSO capability gaps.	**Est. Funding**: Equitable service TOA **Est. Personnel**: Military flag officer and reallocate EMS CFT personnel	Director of EW
As part of a Joint EMSO Office, an EMBM division would enable efforts to develop robust EMS C2, including tools to support real-time spectrum management (e.g., JADC2). This division should focus on selecting a solution for EMBM and promulgating it across the Joint Force. This division would expand EMS C2 to all EW-related capabilities.	**Est. Funding**: Equitable service TOA **Est. Personnel**: A portion of the Joint EMSO office	Director of EW
The DoD must leverage open system architecture to ensure interoperability and compatibility among EW systems and critical data across multiple platforms and service components that are essential to national security.	**Est. Funding**: N/A **Est. Personnel**: Existing personnel **Other**: Industry Partner Open Group, Sensor Open System Group, Modular Open System Approach	Director of EW
Each DoD service should incorporate simulator systems in conjunction with their EW system development. These simulators and training devices should be fielded for use across all echelons of the military and across all domains of warfare.	**Est. Funding**: Costs will vary by program; to be POM'd by acquisition program offices **Est. Personnel**: Existing personnel	OUSD(A&S)
EW system acquisition offices must include requirements for a diverse suite of WARMs both during the development of the system and through routine software updates conducted throughout the life of the system.	**Est. Funding**: Costs will vary by program; to be POM'd by acquisition program offices **Est. Personnel**: Existing personnel	OUSD(A&S) Support from J-8, Joint Staff

Appendix 4: Capstone Analysis

China and the Belt and Road Initiative (BRI):

Short-term and long-term impact on allies, partners, and the United States

What can the United States do to present viable non-BRI options globally?

The Chinese Belt and Road Initiative (BRI) provides an immense amount of funding for major infrastructure projects intended to increase Chinese influence and soft power. Many of the projects are also designed to physically connect China with Asia, Europe, Africa, and the Middle East through a network of roads, railways, ports, and other critical industrial infrastructures. Chairman Xi Jinping incorporated China's Digital Silk Road (DSR) initiative into BRI during his speech at China's first Belt and Road Forum in May 2017, when he insisted that the world "pursue innovation-driven development and intensify cooperation in frontier areas such as digital economy, artificial intelligence, nanotechnology, quantum computing, and advance the development of big data, cloud computing, and smart cities so as to turn them into a digital silk road of the 21st century."[116] Like China's BRI infrastructure, the DSR initiative expands Chinese influence globally by building high-speed communication networks leveraging fiber-optic cables, 5G, satellite systems, and technologies within the electromagnetic spectrum (EMS), providing digital connectivity between the BRI countries. The DSR initiative integrates Chinese influence within international technology standards, directly impacting the EMS domain and maneuver space in which the U.S. and its partners and allies operate.

Consumer dependency on Chinese products and standards, such as autonomous vehicles, telemedicine, and remote work through China's 5G network proliferation, provides a significant advantage to China as it seeks to expand its influence region by region. These Chinese initiatives may achieve significant advantages in the electromagnetic spectrum, allowing the country to collect vast amounts of data and enhance its electronic surveillance regionally and globally. China's increased influence in the EMS bolsters its strategy to become a global leader in emerging technologies and standards. China's continued investment in physical and digital infrastructure projects around the world increases its ability to control communication channels, dictate hardware-software standardization, enable the collection of data, and conduct electronic surveillance. As part of the People's Liberation Army (PLA) information operations forces, China will continue to grow its ability to conduct EW.[117] China's military modernization efforts tie similar lines of funding and policies from civil-military fusion for EW capabilities across the PLA's Ground Force, Navy, Air Force, and Rocket Force.

In the short term, the United States must remain a global leader in setting and enforcing technology standards within the EMS. The United States must leverage its relationships with partners and allies, specifically regional neighbors to China. Collaboration must continue to develop technologies that drive innovation for capabilities and applications for electromagnetic spectrum operations (EMSO) and help define and set operational standards. The United States must prioritize EMSO capabilities that incorporate commercial technologies and that are applicable to dual-use technologies for innovation, such as three-dimensional (3D) sensing and fifth generation (5G) of mobile communications technology, along with maneuvering and preserving spectrum space for U.S. military, national security, and governmental operations. As China builds upon its DSR technologies, China is developing additional capabilities have been innovated, including soft-kill capabilities that will "include jamming; deception; and low-powered, directed energy weapons, high-power directed energy weapons."[118] These DSR technologies may conflict with China's official position that contests efforts to turn outer space into a weapon or a combat zone.[119] The additional congestion within the frequency spectrum generates conflicts, reveals vulnerabilities, and hides emerging Chinese threats for the United States, allies, partners, and other vulnerable global groups.

In the long term, as a counter-option to the Chinese BRI's digital silk road, the United States must build on the extensive array of alliances and partnerships built up since World War II to improve regional integration, increase advanced technology trade, and stimulate economic growth. The United States must champion proven capabilities and technologies, whether they are wrapped into a platform as a part of a fused systems-of-systems or providing a standout interoperable niche item. For example, the F-35 spans over eight program-level partner nations, and nine foreign military sales countries, bringing partners and allies together in the face of global opposition and threats.[120] Not only do the inherent platform capabilities include cutting-edge technologies meant to deliver an advantage during a conflict, but they accomplish strategic objectives that can counter China's BRI when over 1,900 suppliers from over 10 countries partner and contribute to building a platform.[121] Policy-led and partner-shared programs, built at an economic level, contribute to national and global defense capabilities, reduce barriers, and temper global opposition while bringing allies and partners closer during a period of competition in preparation for conflict.

---

[116] Xi Jinping, "Full Text of President Xi's Speech at the Opening of the Belt and Road Forum," Xinhua, 14 May 2017, http://www.xinhuanet.com/english/2017-05/14/c_136282982.htm.
[117] Roger Cliff, "China's Future Military Capabilities," USAWC Press (US Army War College, April 26, 2023).
[118] Cliff, 62.
[119] "China's Space Program: A 2021 Perspective" (State Council Information Office of the PRC), accessed May 3, 2023, https://www.bjreview.com/Documents/202201/t20220128_800274091.html.
[120] Congressional Research Services, "F-35 Joint Strike Fighter (JSF) Program," CRS (Congressional Research Service, May 2, 2022).
[121] Lockheed Martin, "F-35 Lightning II Program Status and Fast Facts," April 4, 2023.

Appendix 5: Acronyms

AFRL	Air Force Research Laboratories
AI	Artificial Intelligence
ARL	Army Research Laboratories
CAPE	Cost Assessment and Program Evaluation
CIO	Chief Information Office
COTS	Commercial-Off-The-Shelf
CTO	Chief Technology Office
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DIU	Defense Innovation Unit
DoD	Department of Defense
DRRS	Defense Readiness Reporting System
EA	Electromagnetic Attack
EAKB	Electronic Attack Knowledge Base
EAR	Export Administration Regulations
ELINT	Electronic Intelligence
EMBM	Automated Electromagnetic Battle Management
EMOE	Electromagnetic Operating Environment
EMS	Electromagnetic Spectrum
EMSO	Electromagnetic Spectrum Operations
EMSSS	Electromagnetic Spectrum Superiority Strategy
EO	Executive Order
EP	Electromagnetic Protection
ES	Electromagnetic Support
EW	Electromagnetic Warfare
EWIR	Electronic Warfare Integrated Reprogramming
FCC	Federal Communications Commission
FFRDC	Federally Funded Research & Development Center
GAO	Government Accountability Office
GOTS	Government-Off-The-Shelf
GPS	Global Positioning System
GTRI	Georgia Tech Research Institute
HIMARS	High Mobility Artillery Rocket System
IC	Intelligence Community
I/Q Signal	Quadrature Signals
IR&D	Independent Research and Development
IT	Information Technology
ITAR	International Traffic in Arms Regulations
JADC2	Joint All-Domain Command and Control
JEMSO	Joint Electromagnetic Spectrum Operations
JP	Joint Publication
JWC	Joint Warfighting Concept
MIT	Massachusetts Institute of Technology
MIT/LL	Massachusetts Institute of Technology Lincoln Laboratories

ML	Machine Learning
NASEM	National Academies of Sciences, Engineering, and Medicine
NASIC	National Air & Space Intelligence Center
NAWC-WD	Naval Air Warfare Center – Weapons Division
NRL	Naval Research Laboratories
NSS	National Security Strategy
NSWC	Naval Surface Warfare Center
NTIA	National Telecommunications and Information Administration
OSA	Open System Architecture
OSD	Office of the Secretary of Defense
OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
OUSD(P)	Office of the Under Secretary of Defense for Policy
OUSD(R&E)	Office of the Under Secretary of Defense for Research & Engineering
P&WPM	Platforms and Weapons Portfolio Manager
R&D	Research and Development
RF	Radiofrequency
SAP	Special Access Program
SCI	Sensitive Compartmented Information
TECHELINT	Technical Electronic Intelligence
WARM	Wartime Reserve Modes