Hudson Institute

MARCH 2021

The Invisible Battlefield: A Technology Strategy for US Electromagnetic Spectrum Superiority

BRYAN CLARK AND TIMOTHY A. WALTON
HUDSON INSTITUTE, CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY

MELINDA TOURANGEAU AND STEVE TOURANGEAU
WARRIOR SUPPORT SOLUTIONS

ABOUT THE CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY AT HUDSON INSTITUTE

Hudson Institute's Center for Defense Concepts and Technology examines the evolving field of military competition and the implications of emerging technologies for defense strategy, military operations, capability development, and acquisition. The center focuses on a comprehensive view: connecting strategy with new operational concepts; assessing the weapons and systems needed to implement new concepts; and evaluating the necessary commitment of resources.

This deliverable is part of Hudson's subcontract agreement with Strategic Analysis, Inc. (no. SA-HUDS-S2MARTS-2020) in support of Navy Surface Warfare Center, Crane Division.

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Fourth Floor
Washington, D.C. 20004

+1.202.974.2400
info@hudson.org
www.hudson.org

Cover: US Marines formed as an Electronic Warfare Support Team (EWST) with 2nd Radio Battalion, II Marine Expeditionary Force Information Group, emplace specially modified bandvagns outfitted with EW equipment alongside Norwegian Army soldiers with Electronic Warfare Company, Military Intelligence Battalion, near Setermoen, Norway, March 14, 2020. (US Marine Corps photo by 2nd Lt. Ben Colyer)

Hudson Institute

MARCH 2021

The Invisible Battlefield: A Technology Strategy for US Electromagnetic Spectrum Superiority

BRYAN CLARK AND TIMOTHY A. WALTON
HUDSON INSTITUTE, CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY

MELINDA TOURANGEAU AND STEVE TOURANGEAU
WARRIOR SUPPORT SOLUTIONS

ABOUT THE AUTHORS

Bryan Clark

Senior Fellow and Director, Center for Defense Concepts and Technology

Before joining Hudson Institute, Bryan Clark was a senior fellow at the Center for Strategic and Budgetary Assessments (CSBA) where he led studies for the Department of Defense Office of Net Assessment, Office of the Secretary of Defense, and Defense Advanced Research Products Agency on new technologies and the future of warfare. Prior to joining CSBA in 2013, Mr. Clark was special assistant to the chief of naval operations and director of his Commander's Action Group, where he led development of Navy strategy and implemented new initiatives in electromagnetic spectrum operations, undersea warfare, expeditionary operations, and personnel and readiness management. Mr. Clark served in the Navy headquarters staff from 2004 to 2011, leading studies in the Assessment Division and participating in the 2006 and 2010 Quadrennial Defense Reviews. Prior to retiring from the Navy in 2008, Mr. Clark was an enlisted and officer submariner, serving in afloat and ashore submarine operational and training assignments, including tours as chief engineer and operations officer at the Navy's Nuclear Power Training Unit.

Timothy A. Walton

Fellow, Center for Defense Concepts and Technology

Prior to joining Hudson, Timothy Walton was a research fellow at the Center for Strategic and Budgetary Assessments (CSBA), where he led and contributed to studies and war games for the US government and its allies on new operational concepts and force planning. Previously, Mr. Walton was a principal of Alios Consulting Group and an associate of Delex Consulting, Studies, and Analysis, both defense and business strategy firms. During this period, he led and supported studies for the US Navy and Army that developed road maps for future technologies, analyzed Asia-Pacific security dynamics, and assessed US and Chinese concepts. He also facilitated strategic planning, capture shaping, and acquisition due diligence for commercial and defense companies.

Melinda Tourangeau

President and Co-Founder of Warrior Support Solutions

As president of Warrior Support Solutions, Mrs. Tourangeau conducts research, studies, and analysis in electronic warfare (EW) and electromagnetic spectrum operations (EMSO) for the Department of Defense. She served in the US Air Force as an electrical engineer managing high technology programs and possesses advanced degrees in engineering and business administration, as well as a patent for a terminal track algorithm for an infrared seeker head, and a provisional patent application on photodiode enhancements using nanotechnology. Mrs. Tourangeau is an accomplished writer, public speaker and business leader, devoted to public service leadership for the greater good.

Steve Tourangeau

Vice President and Co-Founder of Warrior Support Solutions

Steve "Tango" Tourangeau provides premier subject matter expertise to the DoD, industry, and academia on US military electromagnetic spectrum capabilities. Mr. Tourangeau is a nationally recognized EW and EMSO authority backed by experience and a deep understanding of the EMSO landscape for modern warfare concepts and tactics. He is a retired Air Force officer and aviator having served 20 years as a Navigator and Electronic Warfare Officer (EWO) in C-141 Special Operations and F-4D/E aircraft. Since his retirement, Mr. Tourangeau has supported EW capability development for the DoD in various industry roles.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The electromagnetic spectrum (EMS) is a uniquely challenging environment for military operations. Unlike objects physically moving through the air or along the ground or sea, electromagnetic energy travels at the speed of light and cannot be easily contained by walls, boundaries, or exclusion zones. As a result, military EMS activities such as sensing, communications, and electromagnetic warfare (EW) are difficult to separate from one another or from civilian users. The constraints on military EMS access will only grow with the need to allocate spectrum to 5G mobile communications, expanded Wi-Fi coverage, and ubiquitous sensing and communications on vehicles and consumer products.

Adversaries, most prominently the People's Republic of China (PRC) and the Russian Federation, are also countering US military operations in the EMS. They are using passive sensors and jammers to exploit the dependence of expeditionary US forces on active radars for air defense and long-range radio frequency (RF) communications for command and control (C2). As the "home team" in most likely military conflicts, US adversaries can rely to a greater degree on wired communications, multistatic and passive sensing, and their understanding of local conditions to gain an advantage in a highly contested electromagnetic environment.

Addressing challenges to US EMS operations will become more difficult as defense budgets come under pressure from costs to combat the ongoing COVID-19 pandemic, respond to economic recession, and service the growing national debt. Given the growing variety of adversary countermeasures and diverse demands for commercial spectrum, attempting to modify or replace Department of Defense (DoD) EMS systems so they avoid specific threats and civilian encroachments is likely to be unaffordable and continually late to need.

DoD's forecast-centric planning approach, embodied in the Joint Capabilities Integration and Development System (JCIDS), is ill-suited to identify capabilities that solve DoD's EMS challenges in a fiscally constrained and technologically dynamic environment. Forecast-centric planning bases new requirements on the anticipated gaps between capabilities needed to execute desired concepts in future operations and a military force's current or projected capabilities. This analytic approach depends on assumptions regarding the scenarios in which conflict is likely to occur, the capabilities and tactics to be used by opponents, and the probable actions of US allies and partners. The need to make multiple, interdependent assumptions reduces the accuracy of forecast-centric planning, and when assumptions prove incorrect, budget constraints could reduce the force's ability to adapt.

To regain enduring EMS superiority under today's conditions of technological and fiscal uncertainty, DoD will need to adopt a decision-centric planning approach in which adaptability is a more important metric than predicted performance against a particular threat in a specific scenario. In contrast with forecast-centric planning's mobilization of resources to efficiently develop a single solution, decision-centric planning would seek to preserve options for as long as possible within a mission or over a competition. Within operational timeframes, the optionality afforded by a more adaptable force could allow commanders to make faster and more effective decisions, while the complexity imposed on the enemy would degrade its decision-making process. Over strategic and industrial timescales, increasing the adaptability of military systems speeds responses to adversary innovations or enables capability developers to leap ahead of an opponent's advancements.

Adaptability, however, is not sufficient to gain an advantage if the option space is not centered on advantageous capabilities. For example, high-power broadcast radios or scanning search radars can be made highly adaptable using artificial intelligence (AI)-enabled controls, but their risk of counter-detection makes them a poor choice for operations against revisionist powers like the PRC that can deploy numerous distributed passive radiofrequency (RF) sensors in areas where they intend to initiate

conflict. This study will use the technique of net assessment to center the option space for new EMS technologies on areas that exploit fundamental asymmetries between the US military and its main competitors.

Asymmetries

DoD will need to focus its efforts on concepts and capabilities that provide US forces the greatest and most enduring advantages against the People's Liberation Army (PLA) and Russian Armed Forces while mitigating US disadvantages. The net assessment methodology identifies these opportunities based on asymmetries between US and opposing militaries; the asymmetries emerging from this study are described below.

Geography: The PRC and Russian militaries will likely be the home team in future military confrontations, given their ongoing gray-zone operations and stated interests in neighboring countries such as Taiwan for the PRC and the Baltic countries for Russia. As a result, the PLA and Russian Armed Forces can rely to a greater degree than the expeditionary US military on wired communications and can employ passive and multistatic sensors that require multiple networked arrays and a sophisticated understanding of the local electromagnetic operating environment.

Technological innovation: The PLA's concept of system destruction warfare requires development of countermeasures that address specific nodes of US systems of systems. The PLA can leverage the PRC's robust commercial electronics industrial base to develop new capabilities, enabling it to field a comprehensive and changing collection of EMS systems. Russia lacks the PRC's military budgets and fusion with civilian industry, leading the Russian Armed Forces to incrementally adapt existing EMS systems.

DoD largely pursues two tracks in new EMS technologies: new capabilities that are designed to support innovative operational concepts, and improvements to existing systems that counter new adversary capabilities. Because new concepts are not associated with existing major programs, the DoD approach results in the majority of US EMS investment going toward incremental advancements of legacy systems that chase adversary initiatives rather than toward new innovations that create dilemmas for opponents.

Command, control, and communications: The PLA can rely on redundant and resilient communications networks to support a relatively fixed C2 structure of unit commanders, theater commanders, and the Central Military Commission. Russian Armed Forces are more likely to build initial plans and rely on local commanders to execute them, or to improvise when conditions change, or communications are degraded.

The US military exhibits elements of both the PRC and Russian approaches. DoD aspires to create the PRC's level of communications reliability so distant commanders at regional headquarters can manage operations across a theater. Under the concept of mission command, US military doctrine directs local commanders to use their initiative and improvise when communications break down.

Employment of artificial intelligence (AI): The PRC, Russian, and US militaries are all aggressively pursuing AI as an element of their overall force development, but with different priorities for operational systems compared to management and support capabilities. Whereas DoD has prioritized AI incorporation in operational systems, the PLA and Russian Armed Forces have focused AI implementation on C2, management support systems, and intelligence, surveillance, and reconnaissance (ISR).

EMS capability development: As noted above, an asymmetry exists in technological innovation between the PLA's comprehensive systems of systems that target US battle networks, the Russian military's more incremental approach,

and DoD's efforts to modernize existing systems while fielding capabilities for disruptive new operational concepts. This asymmetry extends to each competitor's efforts to develop and field EMS capabilities as well.

Deployment of electromagnetic warfare (EW) capabilities: EW is comprised of electronic attack (EA), electronic support (ES) to monitor the EMS, and electronic protection measures to defend EMS systems from enemy EA. Although the PLA, Russian Armed Forces, and DoD all field operational- and tactical-level EW capabilities through their service branches, the scale and depth of deployment varies significantly. Because of the value they place on EW as an element of their respective military strategies and operational concepts, the PRC and Russian militaries equip units with offensive and defensive EW systems and personnel down to the ground force company, aviation squadron, and naval or paramilitary ship level. US EW capabilities are deployed to varying echelons depending on the service, but generally are held at higher levels of command than in the PLA or Russian Armed Forces.

EMS capability governance: Significant asymmetries exist between the DoD and its competitors regarding the organizations that govern EMS capabilities. The PLA developed a unified governance structure for EMS policy and capability requirements, which parallels the Russian Armed Forces' EW Commander and staff. The US military, in contrast, divides responsibilities for doctrine and strategy between US Strategic Command, the Office of the Secretary of Defense, and the Vice Chairman of the Joint Chiefs of Staff. Moreover, DoD does not give any of these bodies the authority to direct EMS-related spending or acquisition, reducing their ability to implement policy.

Deployment of EW capabilities: EW comprises electronic attack (EA), electronic support (ES) to monitor the EMS, and electronic protection measures to defend EMS systems from enemy EA. Although the PLA, Russian Armed Forces, and DoD all field operational- and tactical-level EW capabilities through their service branches, the scale and depth of deployment varies significantly. Because of the value they place on EW as an element of their respective military strategies and operational concepts, the PRC and Russian militaries equip units with offensive and defensive EW systems and personnel down to the ground force company, aviation squadron, and naval or paramilitary ship level. US EW capabilities are deployed to varying echelons depending on the service, but generally are held at higher levels of command than in the PLA or Russian Armed Forces.

Electromagnetic spectrum operations (EMSO): The US military introduced the EMSO concept to create a coherent framework for EW operations to control the EMS and electromagnetic battle management (EMBM) to coordinate EMS activities such as EW, sensing, and communications. The PRC and Russian militaries do not have publicly released concepts for unified EMS operations, and largely treat EMS control through EW separately from communications, sensing, and spectrum management activities.

Technology Priorities

Technology priorities emerging from asymmetries identified by the net assessment are organized into four main categories: capabilities enabling DoD to obviate, rather than overcome, fundamental challenges; capabilities that undermine adversary advantages; capabilities that turn challenges into opportunities; and capabilities that exploit existing US strengths.

The net assessment methodology accepts risk because it does not attempt to solve every potential future capability gap. This study recommends that DoD EMS systems efforts prioritize the following areas to establish an enduring advantage within a relevant time and the US military's likely budget constraints.

Capabilities to obviate, rather than overcome, fundamental challenges: The PLA's concept of system destruction warfare uses the PRC's fusion of military and civil sectors to create a

comprehensive set of EMS countermeasures designed to target key US battle network nodes and platforms. Continuing to engage in an extended move-countermove competition with the PLA is costly and time-consuming. Therefore, US EMS capability development should focus on adaptive capabilities that can reduce the predictability of US battle network operations.

Capabilities that undermine adversary advantages: The PRC and Russian home team advantage could be countered in part by new technologies that improve the EP capabilities of US forces and reduce their risk of counterdetection. Specifically:

- **Passive and multistatic electromagnetic (EM) sensing:** US forces, as the away team, will need to reduce their EM emissions and signatures across the RF, infrared (IR), and visual spectra to avoid counter-detection and targeting by PRC or Russian forces.
- **Passive and multistatic missile defense:** To reduce the vulnerability of missile defense systems, DoD will need to field passive and multistatic sensors that can detect and track subsonic, supersonic, and hypersonic weapons.
- **Networked ES:** Passive receiving arrays need to securely communicate with one another or with multistatic emitters to enable more precise sensing.
- **Networked EA:** Systems that conduct high-risk EA operations inside contested areas will need to be expendable or inexpensive enough to be attritable. Small and cheap unmanned EA platforms can rely on proximity and coherently combined transmissions to make up for their lower power—an approach that places a premium on secure networking.
- **Low Probability of Intercept/Low Probability of Detection (LPI/LPD) active monostatic sensing:** As an expeditionary force, the US military may have difficulty sustaining multiple passive sensor systems in position to support operations like missile defense, and therefore will need active radars to achieve the necessary precision for engagements. Radars, however, will need features that reduce their likelihood of revealing the defensive system's exact location.
- **Multifunction ES and EA capabilities:** The cost and complexity of using larger numbers of distributed ES and EA vehicles could be reduced in part by ensuring that DoD EW systems are able to perform either sensing or EA operations.

Capabilities that turn challenges into opportunities: As noted above, the PRC and Russian military's focus on potential vulnerabilities of US battle networks could be turned into a disadvantage if US force packages, configurations, and operational concepts are less predictable using technologies such as:

- **Adaptive, wideband EMS systems:** The US military could dramatically accelerate its EMS capability move-countermove cycle by fielding sensor, communication, and EW systems that can operate over multiple gigahertz of frequency spectrum and react to adversary operations in real time by developing and employing new courses of action using AI-enabled algorithms.
- **Automated EW system reprogramming:** Accelerating automated and AI-enabled reprogramming would improve the adaptability of systems that are not yet able to react in real time.
- **Decision support aids and communications management systems:** DoD could turn the challenge of contested communications environments into an advantage by giving junior commanders decision support systems that help them develop courses of action in the absence of connectivity with senior leaders and staffs.

Capabilities that exploit existing US strengths: The US military has adopted new approaches to EW and EMSO, supported by new training and capability integration approaches, that could substantially increase the adaptability and complexity of US operations. These efforts should be accelerated by prioritizing relevant technologies:

- **Virtual and constructive EW/EMSO environments:** The US military could exploit its investments in live, virtual, and constructive (LVC)-based EMSO experimentation and training by accelerating the introduction of virtual and constructive tools and environments at each organizational level, especially at home stations to support ongoing training and experimentation.
- **EMBM systems, including AI:** The US military could capitalize on the PLA's and Russian Armed Forces' lack of EMSO doctrine and exploit the emerging generation of more adaptable EMS capabilities by accelerating the fielding of operationally useful EMBM systems.
- **Open architecture hardware standards:** Combined with a move away from monolithic, multi-mission EMS platforms, increased adoption of open architectures in US military platforms and vehicles would allow use of more modular EMS systems that could be more easily exchanged and modified.
- **Open architecture software tools:** Another approach to open architecture is promoting interoperability between systems. DoD should accelerate the fielding of toolkits like the System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) that build software interfaces on demand to allow disparate networks to communicate.

Conclusion

DoD is at a crossroads in development of EMS-related technologies. The 2020 EMS Superiority Strategy and concepts for EMSO and EMBM advance new approaches to regain an advantage by improving the adaptability of US EMS capabilities both during and between operations. The resulting expansion of options could allow DoD to accelerate or break out of today's move-countermove EMS technology innovation cycle.

Making the shift to more dynamic, agile, and flexible EMS operations, however, will require accepting risk in traditional methods of controlling the spectrum. The US military lacks the time and resources to gain EMS superiority against PRC and Russian forces using a symmetric system vs. system approach. By the time DoD catches up, the PLA or Russian Armed Forces could exploit their EMS advantage to support aggression against their neighbors. DoD's choice is whether to accept continued erosion of its edge in the EMS or to make bold bets on the technologies most likely to circumvent or reverse the inherent advantages enjoyed by its great power competitors.

The technology priorities described in this report represent the US military's best opportunity to establish enduring EMS superiority. They are all being pursued by DoD to varying degrees, but most are merely being sustained rather than accelerated in support of a new approach to EMSO. To reverse trends of the last three decades and give the PRC and Russia challenges to address, funding and attention will need to shift to these new priorities and away from legacy programs that helped win the Cold War.

CHAPTER 1. INTRODUCTION

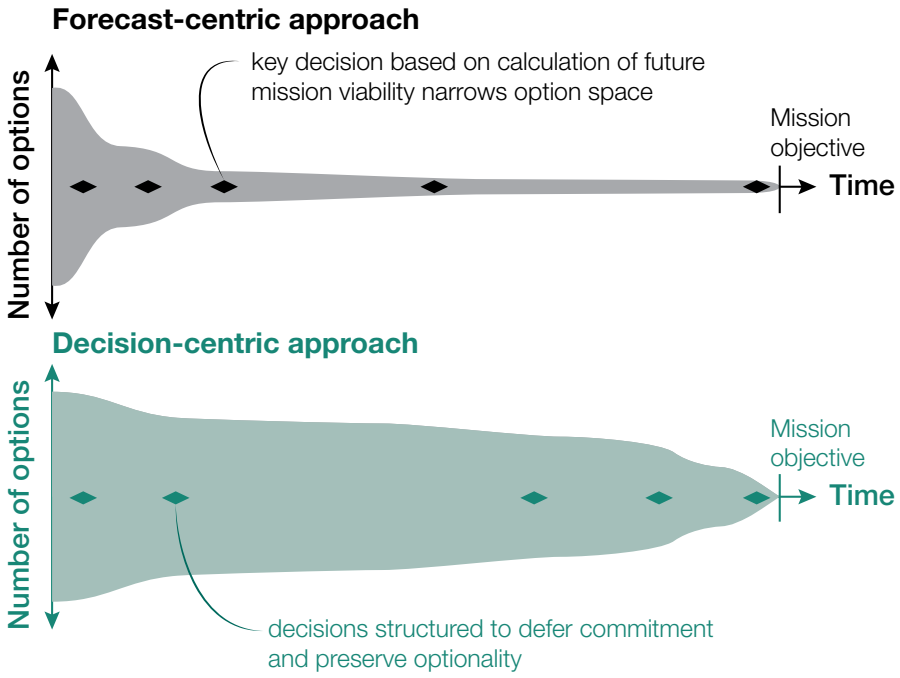
The electromagnetic spectrum (EMS) is a uniquely challenging environment for military operations. Unlike objects physically moving through the air or along the ground or sea, electromagnetic energy travels at the speed of light and cannot be easily contained by walls, boundaries, or exclusion zones. As a result, military EMS activities including sensing, communications, and electromagnetic warfare (EW) operations are difficult to separate from one another or from civilian users. The constraints on military EMS access will only grow with the need to allocate spectrum to 5G mobile communications, expanded Wi-Fi coverage, and ubiquitous sensing and communications on vehicles and consumer products.

Adversaries, most prominently the People's Republic of China (PRC) and the Russian Federation, are also countering US military operations in the EMS using passive sensors and jammers to exploit the dependence of expeditionary US forces on active radars for air defense and long-range radio frequency (RF) communications for command and control (C2). As the "home team" in most likely military conflicts, US adversaries can rely to a greater degree on wired communications, multistatic and passive sensing, and their understanding of local conditions to gain an advantage in a highly contested electromagnetic environment.

Addressing challenges to US EMS operations will become more difficult as defense budgets come under pressure from

Photo Caption: 3rd Armored Brigade Combat Team, 1st Cavalry Division, Electronic Warfare Team, with their new Electronic Warfare Tactical Vehicle. Greywolf is the first brigade combat team (BCT) to receive the new vehicle developed to provide Army Electronic Warfare Teams with the ability to sense and jam enemy communications and networks from an operationally relevant range at the BCT level. (US Army photo by Capt. Scott Kuhn)

Figure 1: Forecast-centric versus decision-centric capability planning



Source: Bryan Clark, Dan Patt, and Timothy A. Walton, *Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage*, (Washington, DC: Hudson Institute, 2021), p. 11.

costs to combat the ongoing COVID-19 pandemic, address the economic recession, and service the growing national debt.[1] Given the growing variety of adversary countermeasures and diverse demands for commercial spectrum, attempting to modify or replace Department of Defense (DoD) EMS systems so they avoid specific threats and civilian encroachments is likely to be unaffordable and continually late to need.

DoD's current forecast-centric planning approach, embodied in the Joint Capabilities Integration and Development System (JCIDS), is ill-suited to identify capabilities that solve DoD's EMS challenges in a fiscally constrained and technologically dynamic environment. Forecast-centric planning bases new requirements on the anticipated gaps between capabilities needed to execute desired concepts in future operations and a military force's current or projected capabilities. This analytic approach depends on assumptions regarding the scenarios in which conflict is likely to occur, the capabilities and tactics to be used by opponents, and the probable actions of US allies and partners. The need to make multiple, interdependent assumptions reduces the accuracy of forecast-centric planning, and when assumptions prove incorrect, budget constraints could reduce the force's ability to adapt.[2]

To regain and establish an enduring advantage under today's conditions of technological and fiscal uncertainty, DoD will need to adopt a decision-centric planning approach in which adaptability is a more important metric than predicted

performance against a particular threat in a specific scenario. In contrast with forecast-centric planning's mobilization of resources to efficiently develop a single solution, decision-centric planning would seek to preserve options for as long as possible within a mission or over a competition.

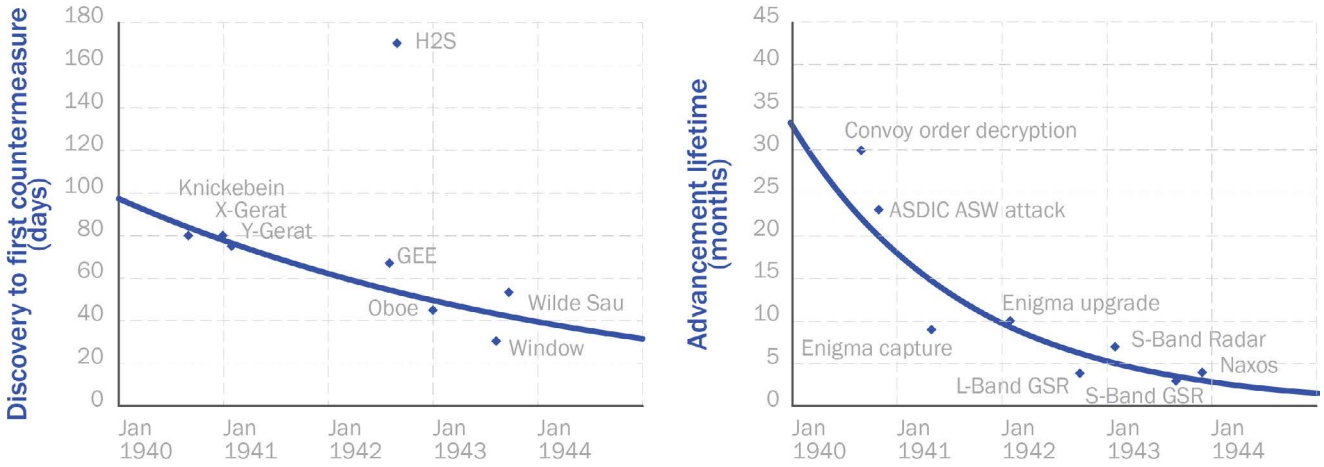
Within operational timeframes, the optionality afforded by a more adaptable force could allow commanders to make faster and more effective decisions, while the complexity imposed on the enemy would degrade its decision-making process. Over strategic and industrial timescales, increasing the adaptability of military systems speeds responses to adversary innovations or enables capability developers to leap ahead of an opponent's advancements.

Winning the Move-Countermove Cycle

Adaptation is a proven path to sustaining military superiority in an extended conflict or confrontation. During World War II, for example, the anti-submarine warfare–submarine competition and bombing campaigns over Germany were won by the Allied powers in part because US and British militaries were able to field a rapidly evolving set of EMS capabilities on their ships and aircraft (figure 2).[3]

DoD is unlikely to repeat the Allied success of World War II with today's generation of platforms and EMS systems. Modern US ships and aircraft are monolithic and highly integrated. Incorporating a new sensor, communication system, or

Figure 2: EMS systems innovation during World War II



Note: Left graph: Knickebein, X-Great, and Y-Great were German radio navigation aids used to direct bombers to targets in the UK; GEE and Oboe were radio navigation aids for British bombers attacking Germany; Wilde Sau was a German air defense fighter tactic; and Window was a British radar-obscuring chaff. Right graph: ASW = anti-submarine warfare; GSR = German Search Receiver; ASDIC = Allied Submarine Detection Investigation Committee. Enigma was a German code machine.

Source: John Stillion and Bryan Clark, *What It Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: CSBA, 2015), https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions.

countermeasure in today's platforms can take years of software development, hull or airframe modification, electromagnetic deconfliction, and procedural evolution—beyond the task of creating the new EMS system itself.

DoD will need to adopt new EMS technologies so it can sustain a lead in the move-countermove cycle against military competitors and with civilian users, and eventually adapt and impose challenges on opponents in real-time. To improve their ability to evolve between operations, EMS systems will need to be increasingly software-based and modular, allowing components or systems to be more easily upgraded or modified to incorporate new techniques and technologies.

DoD's recently released EMS Superiority Strategy supports the importance of adaptability in its central idea that US forces need to maneuver in the EMS to avoid threats, exploit opportunities, and share spectrum with civilian users.[4] The strategy is notable for its emphasis on creating a force that uses agility, battle management, open architecture, and virtual and constructive training systems to achieve freedom of action in the EMS. Each of the strategy's goals pursues this overall approach, as summarized below.

- **Goal 1:** Develop superior EMS capabilities. DoD should create open architecture multifunctional EMS systems that can sense, communicate, and maneuver in the spectrum as directed by electromagnetic battle management (EMBM) systems while avoiding threats and counter-detection through their signal characteristics and maneuver. This method for gaining superiority is different from the attempt to dominate opponents in individual system-versus-system competitions, which was often the model of DoD's post–Cold War EMS capability development.
- **Goal 2:** Evolve to an agile, fully integrated EMS infrastructure. DoD should prioritize better integration and interoperability between intelligence and operational EMS activities to improve responsiveness; the department should also increase reliance on virtual and constructive training to raise proficiency in agile, networked EMS operations without risking adversary intelligence gathering during open-air exercises.
- **Goal 3:** Pursue total force EMS readiness. DoD should professionalize personnel in EMS-dependent fields to enable the career-long development needed for more sophisticated and dynamic EMS operations. To improve unity of effort between EMS specialists and other operators and technicians, the department should incorporate EMS doctrine into force-wide training.
- **Goal 4:** Secure enduring partnerships for EMS advantage. DoD should emphasize interoperability with allies and partners to help ensure that technical advances in DoD EMS operations will not be undermined by other friendly activities. To accelerate the technology improvement cycle, the Pentagon should also enhance its collaboration with industry and professional organizations.
- **Goal 5:** Establish effective EMS governance. DoD should adopt a sustainable governance structure for EMS capability development efforts to ensure the diverse array of EMS-dependent programs and activities is being coherently pursued in support of the strategy.

A key element of achieving EMS superiority and implementing DoD's new strategy will be developing, maturing, and fielding new EMS technologies. Although the EMS Superiority Strategy establishes overall goals and some priorities for technology efforts, these are still broad categories under which a wide variety of science and engineering programs could be pursued. Moreover, the department cannot pursue every potential innovation, and adversaries will continue creating new countermeasures and operational challenges for US EMS operations. This study will assess how DoD should prioritize EMS systems to support the strategy's central idea of EMS maneuver.

A Holistic Assessment

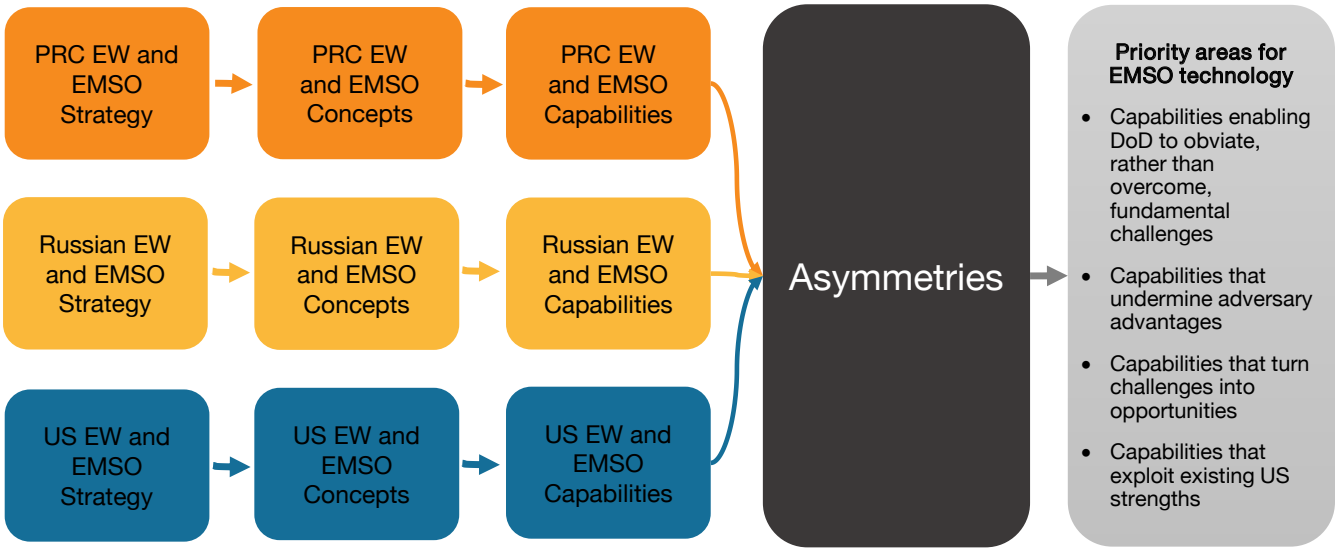
Adaptability alone is not enough to gain an advantage if the underlying capabilities are not effective in the range of potential situations or, in terms of Figure 1, the option space is centered on the wrong set of technologies. For example, high-power broadcast radios or scanning search radars can be made highly adaptable using artificial intelligence (AI)-enabled controls, but their risk of counter-detection makes them a poor choice for operations against revisionist powers like the PRC that can deploy numerous distributed passive radiofrequency (RF) sensors in areas where they intend to initiate conflict.

This study uses a net assessment methodology to help identify the technologies that should defined the option space for DoD EMS capability development. This approach, pioneered by Andrew Marshall, is designed to holistically capture the strategic interactions between competitors and cut through less-consequential details to identify the fundamental asymmetries between them.[5] Although there is no fixed methodology for conducting a net assessment, in general it studies how each subject nation or military plans to compete institutionally and operationally, what means it has for doing so, and how each nation's leaders perceive their position relative to competitors'. To avoid being caught up in contemporary moves and countermoves, a net assessment examines the competitors historically and prospectively for more than a decade in each direction.

Because it encompasses a wide range of quantitative and qualitative information, net assessment is an effective technique to evaluate areas that are not amenable to other methods such as systems analysis or operations research. A net assessment's broad informational and temporal scope can also help lend context and prioritization to competitions that undergo detailed engineering analysis.

EW comprises electronic attack (EA), electronic support (ES) to monitor the EMS, and electronic protection (EP) measures

Table 1: Net assessment methodology used in this study



Source: Figure adapted from Clark, McNamara, and Walton, *Winning the Invisible War*, p. 11.

to defend EMS systems from enemy EA. Electromagnetic spectrum operations (EMSO) combines EW operations to control the EMS with EMBM that coordinates EMS activities including EW, sensing, and communications. The EW and EMSO missions are well-suited to net assessment.[6] Because electromagnetic radiation and its interactions are relatively easy to represent mathematically, EMSO is exhaustively analyzed through modeling and simulation. The specificity and level of detail in these analyses emphasize particular system-versus-system interactions, rather than an overall strategy to enable EMS superiority. The unproductive focus of US capability development on specific systems is further encouraged by the frequent moves and countermoves possible through minor software or hardware modifications in EMS capabilities.

This study will use the net assessment methodology to consider US, PRC, and Russian military EMSO doctrine and institutional, organizational, and capability trends. The asymmetries where one competitor's approach, capabilities, or characteristics could create significant advantages or disadvantages will then be used to identify challenges and opportunities for DoD to address through new EMS technologies (figure 2).

The asymmetries identified through the net assessment will be organized into four main categories designed to focus DoD EMS technology efforts on areas where the investment is most likely to result in an operational advantage in a relevant period of time:

- **Challenges DoD should obviate, rather than attempt to overcome:** These asymmetries create EMSO disadvantages for the US military that cannot be eliminated within likely resource constraints during the next decade. DoD should instead circumvent these disadvantages.
- **Challenges DoD should attempt to alleviate or overcome:** These asymmetries create EMSO disadvantages for the US military that could be eliminated by affordable and achievable technical and conceptual improvements within the next decade.
- **Challenges that could be turned to opportunities:** These asymmetries rely on adversary characteristics that could be turned against the opponent by affordable changes in US EMS capabilities or doctrine during the next decade.
- **Opportunities DoD should more fully exploit:** These asymmetries create advantages for US forces in EMSO but could be enhanced through affordable and executable technical or tactical changes during the next decade.

The technologies associated with the net assessment's asymmetries are where DoD should focus the option space for technology development. Consistent with a decision-centric planning approach, adaptability will be an important characteristic needed in each of these technologies.

The remainder of this study is organized into four chapters that explore the implications of a decision-centric approach to gain EMS superiority. Chapter 2 describes EW doctrine and capability, institutional, and organizational trends for the PRC and Russian militaries. Chapter 3 addresses EMSO doctrine and trends associated with US forces. Chapter 4 describes the resulting asymmetries, and chapter 5 makes recommendations to address the challenges and opportunities organized in the four categories described above.

CHAPTER 2. ADVERSARY ELECTROMAGNETIC SPECTRUM OPERATIONS DOCTRINE AND TRENDS

An important aspect of the net assessment methodology is its emphasis on the interactions between competitors. Analyses that center on US forces, such as those used in capability-based planning, do not help prioritize the most promising programs and can fail to exploit adversary vulnerabilities.[7]

By evaluating the relationship between competitors across multiple dimensions, net assessment is better able to identify opportunities for the US military to gain enduring advantages and mitigate significant vulnerabilities. Moreover, given the steady erosion of the US military's lead in EMS capabilities since the Cold War, US technology development will need to focus more on countering adversary capabilities than on missions where US forces have continued to build on their Cold War advantage, such as undersea warfare.[8]

Photo Caption: Orlan-10 unmanned aerial vehicles during the main stage of the Vostok 2018 large-scale military exercise held by the Russian Armed Forces and involving troops from China and Mongolia, at the Tsugol range. (Photo by Vadim Savitsky\TASS via Getty Images)

PRC

The PRC's People's Liberation Army (PLA) dramatically improved its ability to operate in and control the EMS during the past 20 years through a combination of civil-military fusion, industrial espionage, and robust R&D investment. Although PLA EMS capabilities span the full range of offensive and defensive operations, the PLA's most sophisticated concepts and systems are designed to exploit the PRC's position as the resident power in most potential confrontations, and they focus on the US military as the PLA's chief adversary. By deploying a portfolio of passive and multistatic sensing, wired communications, and specialized EW systems, the PLA intends to dismantle DoD systems of systems and gain an edge in future conflicts.

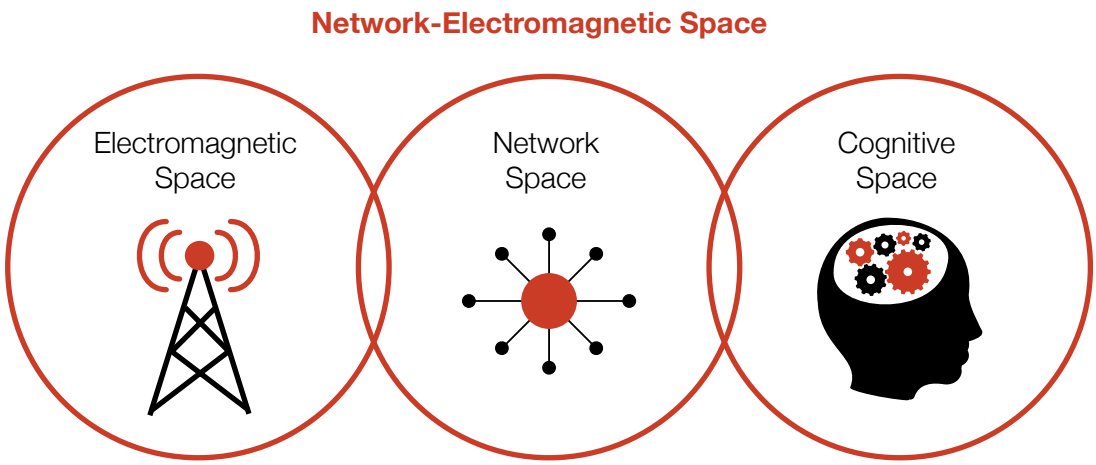
PRC EMSO strategy and operational concepts

PLA doctrine posits that the character of warfare is evolving to make information the dominant element of military power. Under the PLA's concept of informationized warfare, conflict takes place between opposing operational systems in a nonlinear manner across the land, sea, air, space, cyber, electromagnetic, and psychological domains with the goal of defeating the functions of an enemy's systems.[9] PLA forces therefore plan to achieve dominance in systems confrontation by targeting an opponent's information flows.[10]

To wield information power, the PLA developed strategy and concepts for warfare in what it characterizes as a unified network-electromagnetic space (depicted in Figure 4). According to *The Winning Mechanisms of Electronic Countermeasures*, the authoritative strategy written by EW experts from the Electronic Countermeasure Institute (part of the PRC's National University of Defense Technology), the spectrum's significance cannot be overstated since it is the main carrier for information in all domains. *Winning Mechanisms* concludes that whoever controls the EMS will have a potentially decisive advantage in a conflict, and it describes four distinct stages in achieving EMS superiority:[11]

1. **Meticulous planning** to identify forces, systems, and operational approaches that the PLA needs to leverage its strengths while exploiting its enemies' weakness. This

Figure 4: In PLA doctrine, the information environment includes the EMS, cyberspace, and psycological environments



Data Source: J. Michael Dahm, "China: Electronic Warfare," presentation at Hudson Institute EW & EMSO Workshop, July 15, 2020. Figure Source: Authors.

stage relies on accurate intelligence and a comprehensive understanding of enemy capabilities to field countermeasures against each adversary operational system.

2. **Multilevel integration** to provide its own forces with well-timed intelligence. Radar, EO/IR (electro-optical/infrared), and electronic intelligence (ELINT) sensors on land, sea, air and space platforms or systems would be combined to guide the decisions of commanders and operators in fighting jointly. To enable information integration, the PLA's intelligence, information support systems and systems for reconnaissance, surveillance, communications, navigation, position, and guidance must all be hardened and protected against enemy electronic and physical attacks.

3. **Precise release of energy** against "critical nodes" in enemy networks at the outset of an operation. Critical nodes that can lead to the defeat of enemy operational systems differ depending on the opponent but are categorized into five broad groups: reconnaissance and early warning, wireless communication, guidance and fire control, navigation and positioning, and friend-or-foe identification. *Winning Mechanisms* asserts that destroying 10 percent of critical nodes is enough to collapse the enemy's information network. The strategy claims degrading 40 percent of "ordinary" nodes will leave the enemy's network intact, which helps explain why the PLA meticulously studies US military information systems.

4. **Demonstrating effects** to deter further conflict. The PLA's goal is for modern militaries that depend on electronic equipment to self-deter rather than face the PLA's sophisticated electromagnetic strike capabilities and willingness to use them. The PLA also counts on electromagnetic decoy and deception having a psychological impact on the enemy's decision calculus.

The PLA has published two operational concepts that build on *The Winning Mechanisms of Electronic Countermeasures* to describe warfighting in the EMS. Integrated Network EW was introduced in 2002, and the developmental Integrated Information Firepower Warfare concept was first revealed in 2018. The focus of both concepts on EW reflects the separation of EW from communications and sensing in PLA doctrine, whereas in the US military these capabilities are integrated through EMBM as part of EMSO.

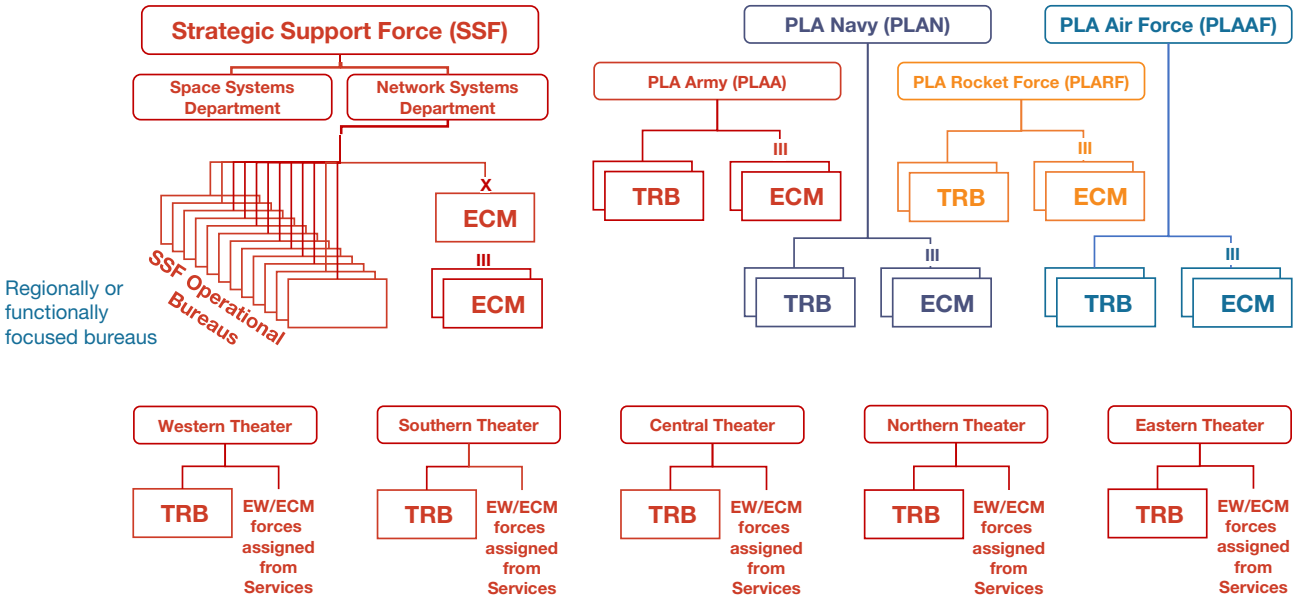
Integrated Network EW combines disruption of enemy information acquisition and transmission using EW with attacks on information processing and decision-making through cyber warfare. The more recent Integrated Information Firepower Warfare concept aims to integrate kinetic and non-kinetic means into a single "information force structure." Integrated Information Firepower Warfare describes a more sophisticated use of EW and cyber systems than Integrated Network EW, including the employment of truly integrated capabilities, such as RF-enabled cyberattacks.[12]

EMSO organization, force structure, and capabilities

The PLA Joint Staff Department's Network-Electronic Bureau (JSD NEB), created as part of a broad set of reforms during 2015, oversees EW and cyber missions across the entire PLA, establishing operational guidance, capability requirements, and rules of engagement for network and electronic countermeasures operations. Consistent with the strategy and operational concepts described above, PLA EW capabilities are organized into Electronic Countermeasures Units, which conduct EW operations, or Technical Reconnaissance Bureaus, which gather intelligence to inform planning and execution of attacks.

The responsibility for developing, fielding, and operating EW capabilities differs between strategic-, operational-, and tactical-level systems (as shown in Figure 5). The PLA's strategic-level EW capabilities are managed and operated by the Strategic Support Force (SSF), formed as part of the 2015 reforms to centralize space, cyber, electronic, and psychological warfare

Figure 5: Organization of PLA EMSO units in SSF and Theater Commands



Note: TRB = Technical Reconnaissance Bureau; ECM = electronic countermeasures. The TRBs have a service or regional focus. The SSF retains strategic EW missions and is a force provide down-echelon.

Source: J. Michael Dahm, "China: Electronic Warfare," presentation at Hudson Institute EW & EMSO Workshop, July 15, 2020.

missions in support of an informationized approach to warfare. Reflecting the PLA's unified view of cyber and EW operations, the SSF is broken into two main departments: the Space Systems Department and the Network Systems Department. The SSF develops, fields, and operates its own EW units and reports directly to the Central Military Commission.[13]

Operational- and tactical-level EW units are provided to Theater Commands by PRC military and paramilitary services. The PLA Army, PLA Air Force, PLA Navy, PLA Rocket Force, People's Armed Police, China Coast Guard, and People's Armed Forces Maritime Militia all field EW capabilities, which are generally developed by the respective services in concert with the PRC's technical bureaus and state-owned enterprises.

The PLA fields diverse, resilient, and redundant electromagnetic systems of systems in support of Integrated Information Firepower Warfare. Whereas US forces use EMSO to capture the interrelated nature of communications, sensing, and EW, the PLA considers EW as a distinct set of capabilities comprising electronic reconnaissance, electronic offense, and electronic defense.[14]

Electronic reconnaissance refers to collecting and analyzing enemy signals, including communication, radar, EO/IR, and hydroacoustic emissions. Electronic offense addresses both electronic and physical attacks against communications, radar, EO/IR sensors, and sonars. Electronic defense focuses on preventing PLA signals from being discovered, identified,

Figure 6: Satellite image and accompanying images of PLA Navy DWL-001 and YLC-29 passive detection and targeting systems (2019)

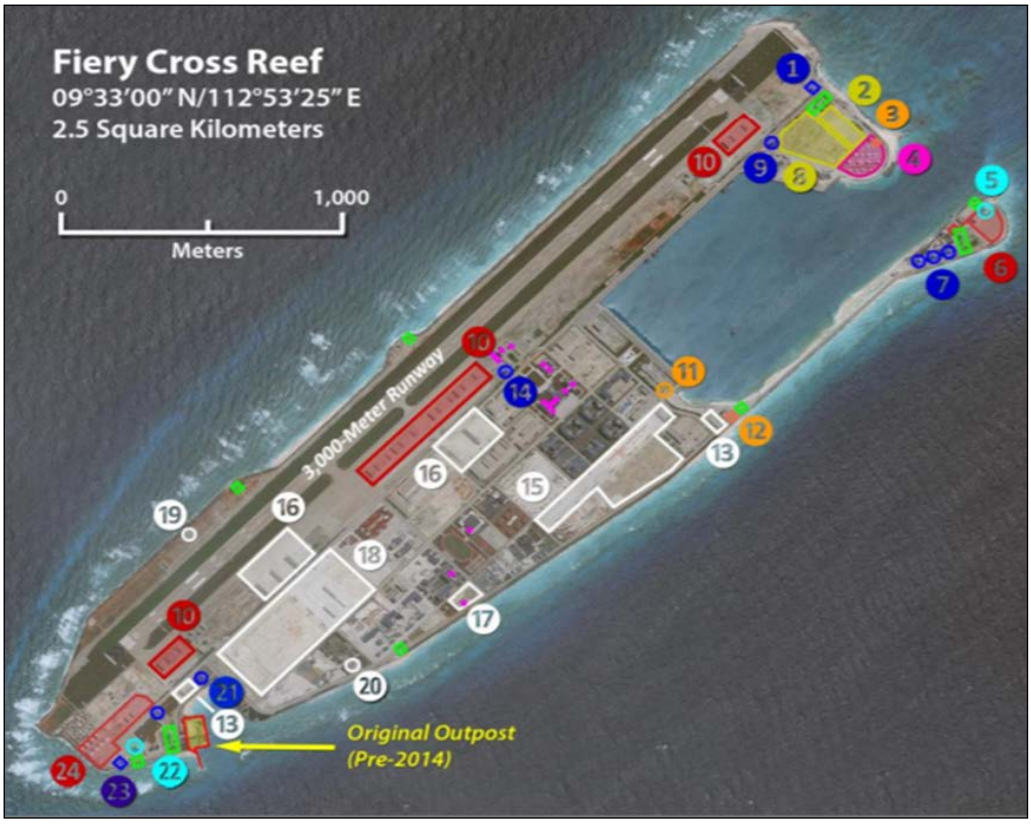
Source: Pir34, Twitter, February 15, 2020, https://twitter.com/pir34/status/1298689227161513991.

or suppressed by an enemy. The range of actions captured under electronic defense is broad, including use of systems like decoys and camouflage to protect radar, EO/IR, and hydroacoustic signatures; electronic counter-countermeasures to protect PLA communications and radar from jamming or detection; and tactics to prevent destruction of EMS systems, such as building fortifications or exploiting terrain and surface features.

Consistent with the concept of system destruction warfare, PLA EW capability development pursues a heterogenous family of systems to disrupt or destroy multiple nodes in an adversary's effects chain and prevent it from being successful.[15] Electronic reconnaissance capabilities exploit the PLA's understanding of local conditions and terrain as the home team to assess the structure of an enemy battle network using widely distributed passive and multistatic RF or EO/IR sensors. For example, PLA Navy DWL-001 and YLC-29 passive detection and targeting systems are used to help protect naval infrastructure and platforms in Hainan, PRC (shown in Figure 6).

To attack enemy battle networks and protect its own systems, the PLA has fielded a comprehensive portfolio of EW capabilities, including kinetic weapons such as anti-radiation missiles, electric weapons such as high-power microwave (HPM) and lasers, suppressive and deceptive jamming, camouflage, multispectral decoys, low observable features, hardening against HPM effects, tactical mobility, and concealment. To PLA

Figure 7: EMS systems and other features on PLA-occupied Fiery Cross Reef



Satellite Communications (SATCOM)
4. SATCOM Earth Station
• Individual SATCOM Dishes

High Frequency (HF) Communications
2. HF Monopole Array (Possible Signals Intelligence)
8. HF Antenna Array

Inter-Island Communications
3. Troposcatter Station North (to Subi Reef)
11. VHF/4G LTE Cell Tower
12. Troposcatter Station East (to Johnson/Cuarteron)

Radar
1. Over-the-Horizon Radar North
7. Air or Surface Radar (3-Tower)
9. Air or Surface Radar
14. Air Traffic Control Radar
21. Air Target Tracking/Air Surveillance Radar (2)
23. Over-the-Horizon Radar South

Electronic Intelligence (ELINT)
5. Probable ELINT Array North
22. Probable ELINT Array South

Offensive-Defensive Strike
6. Surface-to-Surface Missile Facility
10. 24 Fighter Aircraft Hangars (4+16+4)
24. Surface-to-Air Missile Facility

Hardened Infrastructure, Battlespace Management, Concealment
13. Diesel Power Generator Plant (2)
15. Underground Fuel/Water Storage
16. 4 Large Aircraft Hangars (1+3)
17. Meteorology Station
18. Underground Facility
19. Doppler VHF Omnidirectional Range (DVOR) Navigation Beacon
20. Lighthouse/AIS Station
■ Visual Observation Post/Gun Mount

Source: J. Michael Dahm, "A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea: Electronic Warfare and Signals Intelligence," South China Sea Military Capability Series, Johns Hopkins Applied Physics Laboratory, p. 22, https://www.jhuapl.edu/Content/documents/ewandsigint.pdf.

has fielded electromagnetic spectrum management systems improve its C2 of EW operations, although these systems are focused mostly on deconflicting spectrum use rather than coordinating complex offensive operations.[16]

Trends in EMSO posture, training, and operations

In 2006 Hu Jintao, then chairman of the Central Military Commission, delivered a speech highlighting the EMS's importance: "Information dominance is in effect electromagnetic dominance; therefore, we should not only place high-tech weapons and equipment into complex electromagnetic environments to get them trained and tested, but also should carry out comprehensive exercises and drills with tactical backgrounds under such conditions."[17] Hu's speech catalyzed PLA training for operating in complex electromagnetic environments, and mastering the EMS has been a requirement in most military exercises since.

In 2018, the PLA published a new national-level training guidance document, *Outline of Training and Evaluation*, that emphasized realistic and joint training across all warfare domains aimed at "strong military opponents," such as the United States. The missions and tasks addressed by the *Outline* include operations in the EMS.[18] As a result of this guidance, all PLA major exercises now feature significant EW components, including the use of dedicated and capable adversary EW forces.[19] These exercises cultivate operator proficiency and provide opportunities for the development and validation of new concepts and tactics.[20]

The PLA has also enhanced the posture of its EW units by deploying more systems beyond the PRC mainland, where they can impact the ability of US forces to project power in the western Pacific and Indian Ocean. As part of its expeditionary EW operations, the PLA fielded EW systems on vessels and fortifications in the South China Sea, on vessels in the East China Sea, and at the PLA's base in Djibouti.[21] Figure 7 depicts electromagnetic systems on the PLA-occupied Fiery Cross Reef in the South China Sea.

Priorities for future development

The PLA continues to view EMS superiority as essential to future military operations. As part of the 13th Five-Year Plan (2016–2020), the PLA prioritized investment and reform in the areas of "innovative electronics and software," including those relevant to EW.[22] The PLA also intends to improve its cyber and EW capabilities by using artificial intelligence to assist adversary network vulnerability analysis, emitter identification, and electromagnetic spectrum management.[23]

Another PLA priority has been reform of its EW industrial base. In 2015, the PRC adopted a strategy of military-civil fusion, which is "systematically reorganizing the Chinese science and technology enterprise to ensure that new innovations simultaneously advance economic and military development."[24] The PRC can leverage its status as the world's leading electronics manufacturer and exporter, including in new technologies such as 5G, to support a large pool of technical talent, generate internal research and development funding to innovate, and achieve manufacturing economies of scale, all with carryover effects for the PRC's defense sector.[25] Military-civil fusion also aims to leverage theft of foreign technology and international partnerships, in some cases by using front companies or obscuring the military end user from foreign partners.[26]

Digital Hail Information Technology is a representative PRC company that benefited from military-civil fusion, and now describes itself as "China's leader in providing analysis and decision-making support based on data visualization" in the commercial sector. During the past five years, Digital Hail rapidly increased its work for the PLA on cutting-edge decision support tools such as the EMS visualization and planning system shown in figure 8.[27]

The PRC has also sought to reorganize its defense-industrial sector through foreign investments, commercial joint ventures, mergers and acquisitions, and procedural reforms to improve

Figure 8: Digital Hail EMS visualization and decision support tool provided to the PLA

Source: 数字冰雹信息技术 [Digital Hail Information Technology], "航天军工领域 · 成功案例" [Aerospace and military industry: successful cases], https://www.digihail.com/case/casehtjg.html.

weapon system research, development, acquisition, testing, evaluation, and production.[28] Coupled with the PRC's growing comprehensive national power, these efforts collectively suggest that the PLA will likely have the resources and innovation base required to pursue and achieve its EW priorities.

Russia

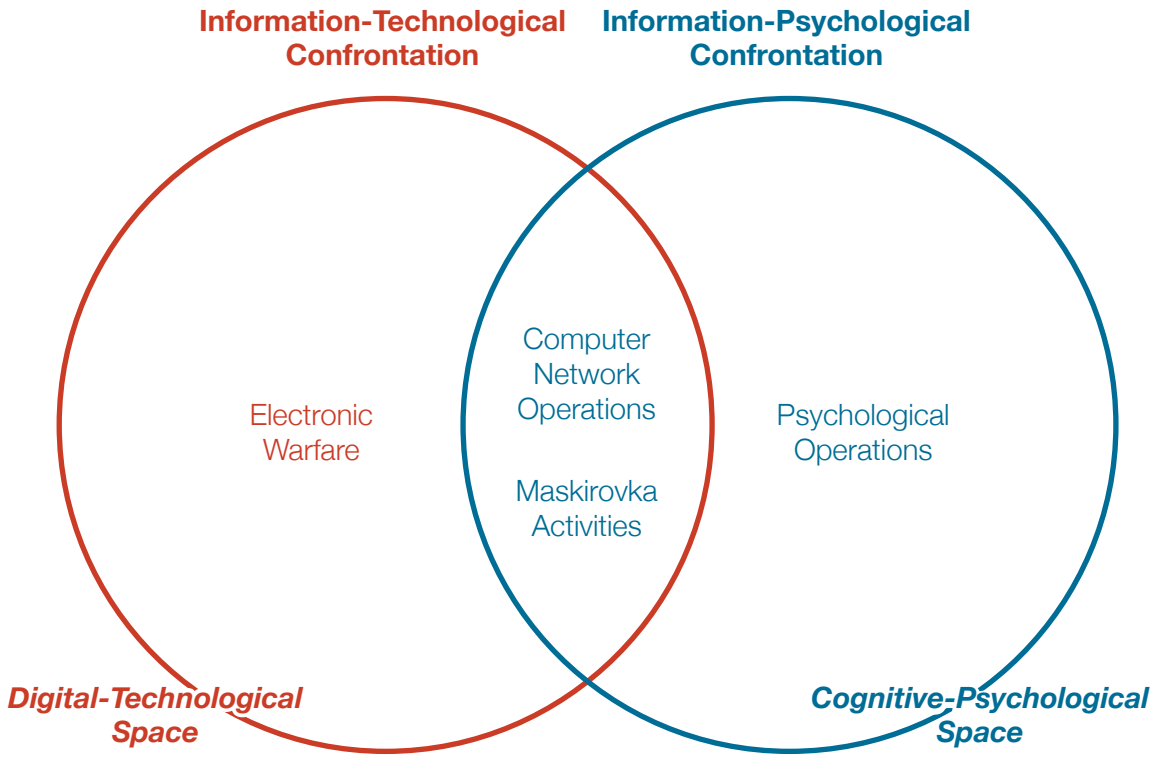
The Russian Armed Forces field a narrower set of EMS capabilities than the PLA. This is partly a function of the smaller Russian economy and military, but also results from Russia's less ambitious military objectives, which are focused on defending the homeland, reducing threats around Russia's periphery, and ensuring access to important sea lanes. Within the missions it pursues, however, the Russian military's EW combat support arm is highly capable, well organized, and guided by a coherent and mature body of strategic and conceptual guidance.[29]

Russian EMSO strategy and concepts of operation

In the decades since the Cold War, Russia's military strategy has evolved to increasingly focus on influencing the information environment and an opponent's decision-making, rather than destroying an enemy outright. Although this evolution aligns well with military investments that are more modest than those of the Soviet Union, the doctrinal change that emerged during the 2010s was grounded in a body of research exploring the growing reach and power of network and electromagnetic communications. The new forms of warfare embraced by Russian military strategy exploit the use of electronic communications to reduce the level of physical violence needed to achieve political objectives and thereby enable military and paramilitary operations to be sustained almost indefinitely.[30]

In a 2013 article titled "The Value of Science Is in Foresight," Russia's Chief of the General Staff, Army General Valeriy

Figure 9: Russian military doctrine views of the information environment



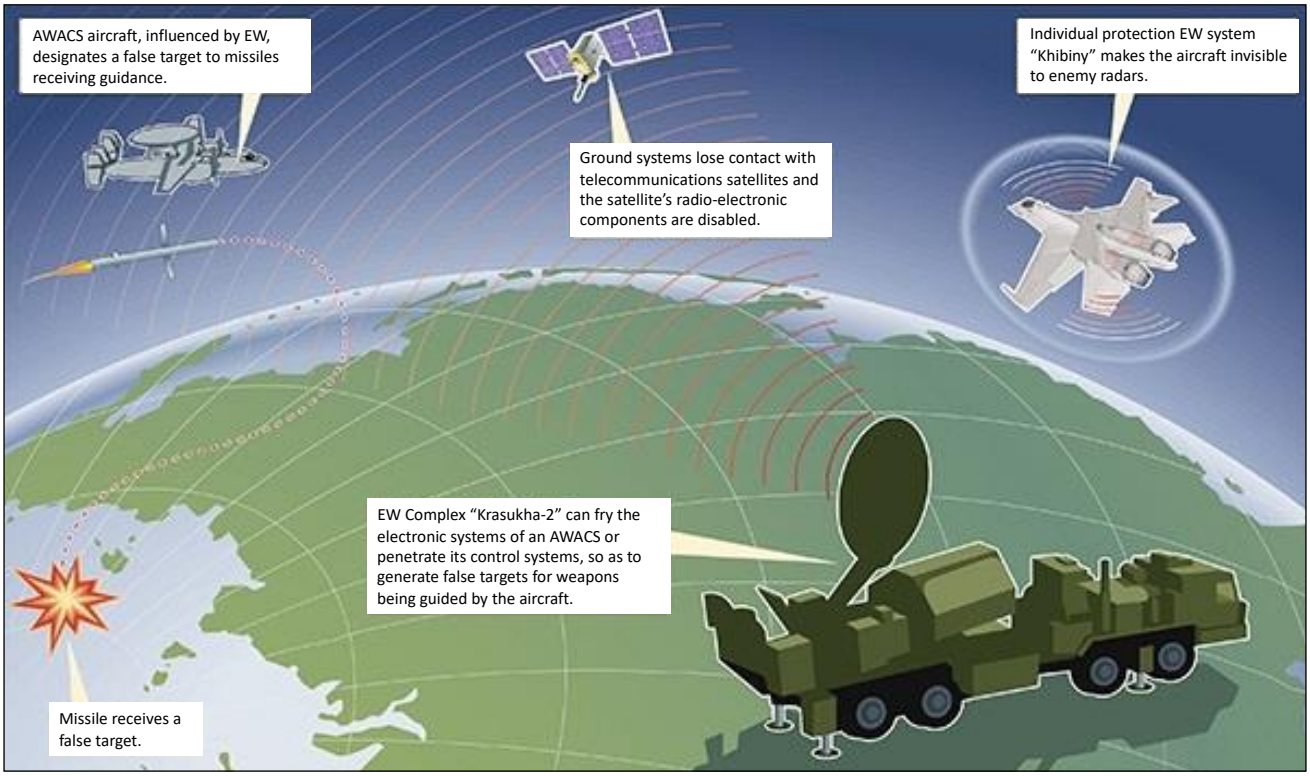
Note: The information environment encompasses technological confrontation in the EMS and cyberspace and psychological confrontation through information operations. These two confrontations merge when the EMS or cyberspace is used to deliver effects designed to degrade an opponent's decision-making, such as computer network attacks that shut down information flows or political messages that sow division in the opponent's society. *Maskirovka* refers to deception activities carried out by the Russian military.

Data Source: J. Michael Dahm, "China: Electronic Warfare," presentation at Hudson Institute EW & EMSO Workshop, July 15, 2020.

Gerasimov, called for rigorous examination of national security challenges and the pragmatic development of solutions that leverage scientific knowledge and employ instruments from across the government—not just the military.[31] Another influential Russian paper, written by Sergei Chekinov and Sergei Bogadanov in 2013 and titled "The Character and Content of New Generation Warfare," aligned with General Gerasimov's analysis of national security challenges and described how modern warfare would draw from different classes of operations, especially EMSO, to achieve military objectives.[32]

Within their concept of New Generation Warfare, these and other Russian military strategists posit the existence of an ongoing information confrontation against foreign and domestic adversaries. The multifaceted confrontation has political, economic, diplomatic, and military dimensions and consists of

Figure 10: Russian depiction of EW forces denying US communications and positioning, navigation, and timing (PNT) across domains as part of radio-electronic attack



Note: AWACS = airborne early warning and control system.

Source: Michael Kofman, "Russian Electronic Warfare," presentation at Hudson Institute EW & EMSO Workshop, July 15, 2020. Overlaid English text translated from Russian by Michael Kofman.

two primary elements: information-technological confrontation and information-psychological confrontation,[33] as shown in figure 9.

New Generation Warfare's information-technological confrontation consists of intelligence operations, EW, and electro-optical and acoustic warfare. Signals intelligence (SIGINT), ELINT, communications intelligence, and acoustic intelligence provide situational awareness needed for effective EW. Forces conduct electronic attack (EA) to suppress, neutralize, or destroy enemy EMS systems, and use electronic protection (EP) to protect friendly EMS capabilities. EW forces operate closely with or are integrated into air defense, rocket, artillery, naval, and space control units, which treat them as force multipliers.

Information-psychological confrontation in New Generation Warfare is waged through individual consciousness, neurological systems, state ideology, and national culture. EMS capabilities are considered essential to information-psychological competition and conflict and would be used to execute effects

such as promulgating disinformation and suppressing or disrupting accurate information.[34]

Russian military operational concepts pursue objectives simultaneously in the information-technological and information-psychological spheres, rather than treating them as distinct phases of a conflict under the purview of separate organizations. For example, Russian cyber operations are used, as during the US 2016 election cycle, to stoke divisions in adversary populations or militaries as part of *maskirovka,* or deception activities.[35] This unified approach also informs Russian recognition that while EW and cyber capabilities are distinct, they are increasingly integrated, as EW provides a means of access for cyber capabilities to target adversary information-psychological spheres.[36]

As with the PLA, Russian Armed Forces doctrine treats communications and sensing as separate activities from EW, and focuses EW forces on EA, EP and associated ES activities that monitor the EMS for threats and opportunities. Under Russian doctrine, concepts for EW should implement a systemic approach to supporting Russian battle networks and targeting adversary information flows; achieve unity and hybridity of effort by integrating various combinations of EW and non-EW capabilities; and sustain a permanent, scalable campaign that can conduct operations across the range of conflict. These characteristics are reflected in four primary Russian EW concepts of operation, listed below.[37]

- **Radio-electronic attack:** Destroying adversary weapons physically or through non-kinetic actions using EA, directed energy, or cyber operations, with the goal of creating a "disorganizing strike" that suppresses an enemy's ability to coordinate and conduct complex operations (figure 10)
- **Radio-electronic protection:** Protecting forces against enemy information-enabled attacks, including but not limited to adversary EA
- **Countermeasures against reconnaissance:** Using emissions control and information assurance activities to guard against adversary reconnaissance
- **Radio-electronic information support:** Providing ELINT, SIGINT, acoustic targeting, and cyber penetrations to support precision targeting against adversary forces

Russian combat in Chechnya, Georgia, Ukraine, and Syria has provided lessons to inform the maturation of existing concepts and development of new doctrine. These operations—especially in Ukraine—reinforced the centrality of information to military campaigns and stimulated a shift in the Russian military's EW operations from information denial toward deception.

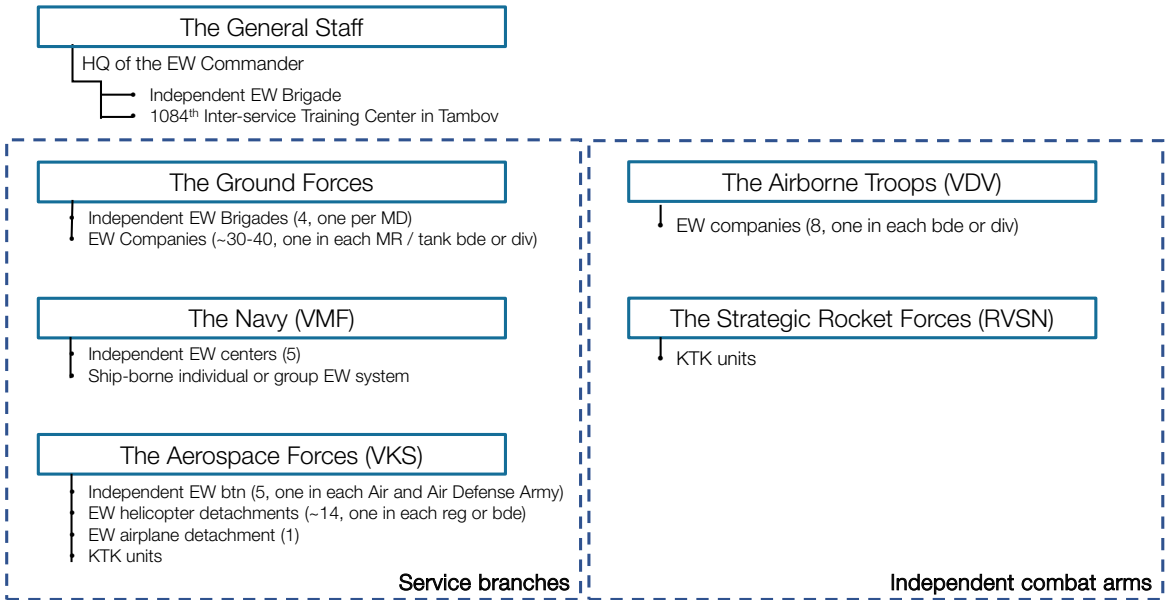
Organization, force structure, and capabilities

As part of a series of military reforms, the Russian Armed Forces in 2009 established the Electronic Warfare Force, elevating the status of EW units from a combat support element to a combat support arm on par with Military Engineers or Signal Troops.[38] An EW Commander was also established within the General Staff, increasing the EW community's bureaucratic influence.[39] Currently, Russian EW forces are divided into three classes of units:[40]

1. EW units of the armed forces' services and independent combat arms, as shown in Figure 11. These forces provide tactical or operational level EW support to Russian military district commanders and are organized into EW brigades for the Ground Forces, EW companies of the Airborne Troops, EW battalions or detachments in the Aerospace Forces, and shore-based EW centers or systems on ships and aircraft.[41]

2. A network of units and systems throughout the Russian Armed Forces for Comprehensive Technical Control (KTK), a Russian term for passive EMS monitoring. The KTK network focuses on two primary tasks throughout competition and conflict: emissions control to reduce the risk of counter-detection, and spectrum management to promote interoperability and deconflict EMS activities. More

Figure 11: Overview of EW unit organization in Russian Armed Forces



Note: Russia's strategic jamming system are not included in diagram. bde = brigade; btn = batallion; div = division; Ind = independent; KTK = Comprehensive Technical Control MD = military district; MR = motorized rifle; reg = regiment.

Source: Jonas Kjellén, "Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces," Swedish Ministry of Defence, 2018, p. 34, https://www.foi.se/rest-api/report/FOI-R--4625--SE.

recently, KTK units have been tasked with "Protecting State Secrets"—that is, with preventing enemy exploitation of civilian or commercial electronic communication devices and systems, such as smart phone and other mobile devices.

3. EW assets of the strategic radio-jamming system. In addition to executing EA against adversary communications, these systems conduct SIGINT and ELINT across theaters to support Russian intelligence operations.

The Commander of the Electronic Warfare Force oversees the Electronic Warfare Force and has one independent EW brigade and the 1084th Training Center in Tambov under his direct command.[42] The Russian Armed Forces' service branches (Ground Forces, Navy, and Aerospace Forces) and independent combat arms (Airborne Troops and Strategic Rocket Forces) command their own EW units in accordance with direction from the Commander of the Electronic Warfare Force.[43]

Russian EW forces field systems able to detect and engage targets on the ground, at sea, in the air, and in space, most prominently the Murmansk-BN, RB-109A Bylina, and Leer-3. The Murmansk-BN is an electronic surveillance and attack complex consisting of seven trucks with 32-meter-high

antennas capable of monitoring and jamming communications and sensors in the high frequency/very high frequency/ultra high frequency (HF/VHF/UHF) bands.[44] With a reported range of up to 5,000 kilometers, the system is capable of disrupting satellite or airborne communications and sensors.[45] Murmansk-BN systems can be networked across the nation to support Russia's National Strategic EW System.[46]

The RB-109A Bylina is an EW system mounted on five trucks that conducts command and control of EW systems at the brigade level.[47] The Bylina system is reported to have an AI-enabled C2 algorithm that facilitates automated decision-making by assessing the EMS, configuring electronic surveillance activities by its own and other units, and commanding the execution of electronic attack by other units while minimizing potential adverse effects on friendly communications and radar systems. The system is controlled by human operators at brigade headquarters, providing a human-on-the-loop capability. Procurement of the Bylina started in 2018, with a goal of outfitting all EW brigades by 2025.

The Leer-3 consists of a mobile vehicle command post that controls three Orlan-10 unmanned aerial vehicles (UAVs).[48] The UAVs are equipped with RF receivers and transmitters capable of jamming mobile phones and some radios, geolocating signals, and transmitting SMS messages to mobile phones. The system provides units with the ability to conduct relatively low-power electronic attacks over local areas, with the command post controlling the UAVs. The ability to transmit SMS messages also provides an opportunity to target an adversary's information-psychological sphere by deceiving or demoralizing adversary forces and civilian populations. Russian forces are experimenting with other, larger UAVs capable of operating over longer distances and targeting a wider range of radio frequencies.

Russian Armed Forces services and independent branches also employ EW systems for self-protection on platforms and for area effects. In addition to EW systems on its platforms, the Russian Navy operates ground-based EW systems to "assess the electromagnetic spectrum, instantly detecting, analyzing, and locating radio signals in conjunction with other mobile and SIGINT/ELINT systems, as well as using software, electronic, and other decoys to divert and misdirect enemy platforms and systems away from intended targets."[49] The Russian Navy has also fielded ground-based EW jammers to defend key bases and supplement existing Murmansk-BN mobile EW systems.[50] The Russian Air Force similarly has EW self-protection systems on board its aircraft and ground-based EW systems to defend its bases.

Future modernization of Russian EW forces will reflect four main trends. First, units will become more mobile, with systems usually mounted on trucks or armored vehicles, and capable of quickly operating once stationary, or in some cases while on the move.[51] Second, EW units will become more highly integrated with other forces, either operating as part of other units or closely coordinating with them.[52] Third, Russian EW forces will increasingly incorporate capabilities outside of traditional RF sensors, radios, and countermeasures such as EO/IR, laser, and HPM systems.[53] Fourth, Russian EW forces will become more automated, incorporating AI to improve their ability to anticipate and react to adversary actions in the EMS.[54]

Trends in posture, training, and operations

Russian military forces are primarily based within the country, with a small number deployed outside of Russian territory. The Russian Ground Forces have five EW brigades concentrated in the western portion of the country, reflecting the national focus on countering NATO forces. Smaller EW units are distributed across the country and co-located with major bases and critical infrastructure.

Additional EW forces are deployed outside of Russian territory on naval units and in Ukraine's Crimea, which is currently occupied by Russia, as part of a so-called "electronic bastion."[55] Moreover,

a wide range of sub-battalion-strength EW forces have been deployed to separatist-occupied portions of Ukraine, Syrian government–controlled areas in Syria, and possibly Libya.[56]

The Electronic Warfare Force has instituted a rigorous program of technical training and exercises to maintain EW unit proficiency, complemented by experience gained during Russian combat operations. The Electronic Warfare Force Headquarters leads training of EW specialists and officers serving in EW units using the 1084th Inter-service Electronic Warfare Training Center in Tambov and the Fifth Academy at Vornezh.[57] Training consists of classroom and field instruction, supported by advanced computer simulators.[58] Overall, the Electronic Warfare Force aims to produce highly skilled operators, but faces challenges in selecting candidates with sufficient academic credentials and aptitude and graduating enough to meet operational needs.

By 2012 the Russian Electronic Warfare Force was sufficiently organized and proficient following its reforms to begin a series of frequent, large-scale exercises.[59] EW units in services and combat-support elements also conduct regular smaller-scale exercises to evaluate new EW tactics and test integration with other units.

Beyond exercises, ongoing combat operations in Ukraine and Syria provide operators with experience and stimulate conceptual and capability innovations. Russian EW assets jam and intercept fixed and mobile radio and mobile phone communications, target Ukrainian UAVs by jamming controller or GPS signals, disrupt radio-fused munitions from artillery and mortars, and geolocate electromagnetic emissions to support kinetic targeting.[60] Notable innovations during the conflict in Ukraine include the use of highly mobile, distributed independent tactical EW groups to avoid counter-targeting and the incorporation of new EW algorithms and automated C2 systems.[61] Lessons learned from the large-scale employment of EW forces in Ukraine have been incorporated into a new General Staff–issued EW manual published in 2017.[62]

Russian military forces employed EW systems in Syria for airbase defense and self-protection and jamming by Su-30SM, Su-34, and Su-35S aircraft. Russian EW forces also employed Leer-3 in Syria, where it jammed enemy communications networks and sent false SMS messages to mobile phones in support of Syrian Army operations.[63]

Priorities for future development

EW is a focus of Russian Armed Forces modernization, with actions divided between organizational, capability, and industrial lines of effort.[64] Organizationally, senior Russian defense officials have suggested three chief priorities. First, the number of skilled soldiers serving in EW units should continue to increase.[65] Second, training should continue to intensify in quality and scale.[66] Third, the Russian Electronic Warfare Force should continue to stand up the Electronic Warfare Situational Center, which will automatically integrate information from across EW units.[67]

The best indication of capability development priorities is a 2017 interview by Major General Yuriy Lastochkyn, Commander of the Russian Electronic Warfare Force.[68] In the interview, he identified five areas for force development. First, the force should develop small jamming modules that can be carried by a range of UAVs and can achieve controlled effects. Second, the force should develop systems capable of destruction using powerful electromagnetic radiation, both through mobile platforms that emit the electromagnetic radiation (such as high-power jammers, HPM, and lasers) and through specialized ammunition (such as explosive-driven HPM systems).[69] Third, the force should develop techniques to counter adversary command and control systems by influencing the accessibility, integrity, and confidentiality of information.[70] Fourth, the force should introduce new techniques to spoof electronic signals and deceive adversary units, weapons, and C2 complexes.[71] Fifth, the force should increase its overall level of information security and improve algorithms that enable unified C2 of EW and other units.[72]

Another area of research emphasis for Russian EW forces is systems capable of locating targets through new or improved phenomenologies that have a low probability of being counter-detected. This includes the development and fielding of new passive, distributed radar systems that cue or have been integrated into air and missile defense architectures, the development of new photonics radars that combine optical and microwave elements, and new EO/IR systems.[73] Additionally, Russian forces seek to integrate multi-domain Identification Friend or Foe (IFF) systems with EW systems, facilitating unified command and control across the EMS.[74]

In terms of industrial priorities, the Russian Armed Forces seeks to cultivate a domestic civil-military ecosystem that can meet and exceed conceptual and technical demands.[75] It has instituted a series of reforms to stimulate innovation and transition the electronic warfare industrial base from one heavily reliant on Soviet-developed technologies to one that uses, develops, and can effectively produce new technologies. In support of this, the Russian military created a new academic institute, the Fifth Faculty, at the Zhukovsky-Gagarin Air Force Academy. The Fifth Faculty is tasked with the "preparation of highly qualified specialists in the domain of EW and Informational Security" and serves to consolidate academic intellectual development of both commissioned officers and civilian scientists at a center of excellence.[76]

The Russian Ministry of Defense has also focused EW development and production work at two state-owned, vertically integrated companies: KRET and Sozvezdie.[77] This consolidation reduced overhead expenses and concentrated valuable engineering skills (Russia, like the United States, faces a shortage of young engineers); it also improved EMS system compatibility by aligning standards within and across companies.[78] These industrial efforts have helped to offset limited production runs on new systems and the effects of Western sanctions on Russia, as well as the loss of Ukraine as a source of systems and components.[79] The reforms have also facilitated the unified marketing of EW systems suitable for exports, which are needed to complement domestic orders.

Summary

The PRC and Russian militaries embrace strategies that view the information environment as the main battlefield for future confrontation and conflict. Both competitors implement their information-centric strategies through concepts that pursue decision-making superiority primarily through EW, using ES to assess US battle networks, EP to defend adversary command, control, and communications (C3), and EA to degrade carefully identified US vulnerabilities. To operationalize this approach, the PLA and Russian Armed Forces established EW units at the national and regional levels, supported by organizations within each of their service branches that train, equip, and sustain EW forces.

The US military will face significant challenges in countering the comprehensive array of EW capabilities and forces fielded by the PLA and Russian Armed Forces. As discussed in the next chapter, EW and EMSO units are distributed throughout the US military, but the systems they employ are not widely diverse and remain in service for decades. The PRC and Russian militaries can exploit the relatively static nature of US EMS capabilities to field countermeasures that degrade US battle networks. Regaining an advantage by simply fielding new counter-countermeasures to PLA or Russian EW systems may be unaffordable within projected US defense budgets and take too long to be operationally relevant. A new set of operational approaches and technologies is needed for US forces to regain their advantage in the EMS.

CHAPTER 3. US TRENDS IN ELECTROMAGNETIC WARFARE AND ELECTROMAGNETIC SPECTRUM OPERATIONS

Multiple assessments during the last decade found that the US military is falling behind its potential opponents in the competition for EMS superiority.[80] DoD and the US Congress responded to the perceived erosion of US EMS capability with increased investment, new governance structures, and new operational concepts that combine EW and EMBM under EMSO.[81] These efforts, however, largely build upon the post–Cold War assumption of US military predominance. New US concepts establish objectives of gaining unfettered access to the EMS while denying it to others at will, and the majority of EMS spending goes to improved versions of existing radars, radios, and EW systems that attempt to mitigate the impact of adversary countermeasures.

The US military is unlikely to experience or create a permissive EM operating environment against modern, well-organized,

Photo Caption: Staff Sgt. Alex Garviria, 721st Communication Squadron senior systems controller, and 2nd Lt. Rachel James, 721st CS crew commander, work in the Global Strategic Warning and Space Surveillance System Center at Cheyenne Mountain Air Force Station, Colo., Sept. 2, 2014. (US Air Force photo by Airman 1st Class Krystal Ardrey)

and proficient militaries such as those of the PRC or Russia. Moreover, as commercial EMS capabilities become more sophisticated and military systems proliferate, smaller powers such as Iran or North Korea will be able to conduct network-centric operations and degrade US military access to the EMS in their regions.

To regain its ability to operate effectively in the EMS, US forces will need to mount a new approach that does not presume EMS dominance for its success. The recently released DoD EMS Superiority Strategy marks a move in that direction, which is supported by some new trends in US EMS capability development, as described below. Overall, however, DoD EMS systems efforts do not prioritize the most impactful attributes needed to excel and eventually to obviate the move-countermove cycle: software-based, modular systems able to conduct networked, distributed EMS operations with maneuverability and agility across the EMS.

This chapter describes and evaluates US EMSO strategy and capabilities using the same categories as in the previous chapter on the PRC and Russia.

US Strategy and Concepts of Operation

The 2018 US National Defense Strategy (NDS) argues that the United States is in a long-term competition with the PRC and Russia, and that to deter and defeat adversary aggression DoD must build a more lethal force.[82] Notably, the NDS does not prioritize EMSO, and its emphasis on lethality implies that the US military will succeed primarily through physical actions and attrition against the enemy, rather than deception, disruption, and maneuver.

The NDS's strategic direction is consistent with approaches taken by US forces during post–Cold War conflicts in Iraq, Afghanistan, Kosovo, and Libya where the US military was invading or imposing costs on an opponent to change the status quo. In confrontations against the PRC or Russia, US forces are likely to instead be attempting to uphold the status quo. Given the capability and proximity of the PLA or Russian Armed Forces to potential targets of aggression such as Taiwan or Ukraine, respectively, US forces may not be able to impose sufficient attrition to prevent the aggressor's success. Moreover, as described in the previous chapter, PRC and Russian strategies prioritize competition in the information environment and employ gray-zone or sub-conventional means of achieving objectives, rather than large-scale armed aggression. DoD will likely need new strategies to deter or defeat PLA and Russian Armed Forces in the emerging information-centric competitive environment.

Although it acknowledges the growing importance of decision-making, rather than attrition, to succeed in 21st century conflicts, DoD's Combined and Joint All Domain Command and Control (CJADC2) initiative reflects the US military's traditional emphasis on overcoming EMS access challenges to conduct C2 and coordinate fires across an operational theater. Emerging from Army and Air Force efforts to improve all-domain C2, CJADC2 is a construct for organizing programs that enable communications connectivity between military units and dynamic C2 of their operations in support of DoD's emerging Joint All-Domain Operations (JADO) operational concept.[83] Service-led initiatives supporting CJADC2 include the Air Force's Advanced Battle Management System (ABMS) for C2 and the Army's Project Convergence and Navy's Project Overmatch for interoperability and decision support.[84]

CJADC2's goal of connecting sensors, shooters, and commanders over wide areas may not be achievable against robust and improving Russian and PRC EW capabilities. US forces will therefore increasingly depend on mission command, in which junior leaders take command of their subordinate units when communications are lost with higher headquarters.[85] Junior commanders, however, will be unable to exploit their initiative and creativity unless DOD pursues a more holistic C3 approach in which communications investments are

balanced against those for C2 tools.[86] Although ABMS, Project Convergence, and Project Overmatch are developing some decision-support systems, the emphasis in these initiatives has been connectivity and inoperability.

DoD's 2020 EMS Superiority Strategy begins the US military's shift away from attempting to achieve EMS dominance over wide areas in its central idea of using maneuver and agility in the EMS to avoid threats, create challenges for opponents, and enable spectrum sharing between military and commercial users.[87] This approach could support CJADC2 thorough the strategy's five main goals:

- **Goal 1: Develop superior EMS capabilities.** DoD should create open architecture multifunctional EMS systems that can sense, communicate, and maneuver in the spectrum as directed by EMBM, while avoiding threats and counter-detection through their signal characteristics and maneuver. This method for gaining superiority is different from the attempt to dominate opponents in individual system-versus-system competitions, which was often the model of DoD's post–Cold War EMS capability development.
- **Goal 2: Evolve to an agile, fully integrated EMS infrastructure.** DoD should prioritize better integration and interoperability between intelligence and operational EMS activities to improve responsiveness; the department should also increase reliance on virtual and constructive training to raise proficiency in agile, networked EMS operations without risking adversary intelligence gathering during open-air exercises.
- **Goal 3: Pursue total force EMS readiness.** DoD should professionalize personnel in EMS-dependent fields to enable the career-long development needed for more sophisticated and dynamic EMS operations. To improve unity of effort between EMS specialists and other operators and technicians, the department should incorporate EMS doctrine into force-wide training.
- **Goal 4: Secure enduring partnerships for EMS advantage.** DoD should emphasize interoperability with allies and partners to help ensure that technical advances in DoD EMS operations will not be undermined by other friendly activities. To accelerate the technology improvement cycle, the Pentagon should also enhance its collaboration with industry and professional organizations.
- **Goal 5: Establish effective EMS governance.** DoD should adopt a sustainable governance structure for EMS capability development efforts to ensure the diverse array of EMS-dependent programs and activities is being coherently pursued in support of the strategy.

US operational concepts do not reflect the strategy's reliance on maneuver for achieving EMS superiority. However, the 2020 version of Joint Publication 3-85 on joint electromagnetic spectrum operations improves upon predecessor concepts by integrating communications, sensing, and EW through EMBM, providing a common reference and framework for different service units operating under combatant commanders.[88]

Joint Publication 3-85 also advances a new framework to establish requirements for EMS access based on real-time needs for friendly or adversary sensing and communications, rather than pursuing EMS dominance, in which US forces can access and operate in the EMS on demand while denying access to enemies at will.[89] For example, US forces may need to persistently search for enemy units using low-fidelity passive RF and EO/IR sensors and if necessary conduct short-duration active radar operations for targeting. In some cases, surveillance and targeting could be conducted completely using passive EM sensors. The only communications required could be cueing messages among sensors and a targeting message to the weapons platform. Achieving this level of EMS access could be attained with a combination of agile radars and radios with EM decoys to distract adversary electronics intelligence and jamming.

Within their own doctrine, US military services all treat EMSO as a subset of information warfare, along with intelligence, cyber, information operations, and in some cases meteorology and oceanography.[90] They each, however, take a distinct approach to incorporating EMSO into their overall service concepts.

The US Army's Multi-Domain Operations (MDO) concept plans on employing distributed and noncontiguous capabilities across domains to conduct fires and maneuver that disintegrate enemy formations.[91] This concept relies on cyber electromagnetic activities (CEMA) to degrade and defeat adversary forces through EMSO.[92] As described by the Army's Concept for Cyberspace and Electronic Warfare Operations, CEMA includes cyberspace operations, communications, EW, spectrum management, intelligence, and information operations.[93]

The US Navy's Distributed Maritime Operations (DMO) concept directs the use of distributed formations and EW to enhance the survivability and lethality of naval forces and increase complexity for adversaries.[94] The Navy complements this concept with the Electromagnetic Maneuver Warfare (EMW) concept, which marries maneuver in the maritime, air, and space domains with agility in the EMS. The Navy implements EMW through a series of guides and manuals describing warfighting approaches in the EMS.[95]

The US Marine Corps Expeditionary Advanced Base Operations (EABO) concept directs Marines to conduct mobile and distributed operations ashore to provide fires, intelligence, surveillance, reconnaissance, and targeting (ISR&T), EW, and ground support to the overall naval force.[96] Under the Marine Corps approach, EMS systems of systems can be employed to create scalable distributed effects that establish battlespace control.

The Department of the Air Force's doctrinal annex on its role in Joint All-Domain Operations recognizes the contested nature of the EMS and calls for synchronizing and integrating the targeting cycles of all the operating domains and the EMS.[97] Additionally, the Air Force's doctrinal annex on EW and EMSO specifies the organization, planning, and execution of EW and EMS operations.[98] The Space Force's seminal doctrine publication, "Spacepower," recognizes the dependence of space operations on the EMS and calls for services to require specialization in space electromagnetic warfare to exploit and defend EMS access.[99]

In summary, DoD EMS strategy is improving toward a more decision-centric approach that relies on maneuver and agility to deny adversaries effective information while sustaining necessary situational awareness, targeting, and communications for US forces. In service-specific doctrine, however, information superiority is primarily treated as a means to enable efficient fires, rather than as a way to directly achieve battlefield advantage. US operational concepts will need to evolve to reflect DoD's new EMS Superiority Strategy.

Organization, Force Structure, and Capabilities

Responsibilities for EMS forces and capabilities are diffused throughout DoD. The Vice Chairman of the Joint Chiefs of Staff (VCJCS) is the Senior Designated Official responsible for EMSO within DoD and leads the EMSO Cross-Functional Team (CFT). With the DoD Chief Information Officer. With the Undersecretary of Defense for Acquisition and Sustainment, the VCJCS oversees the EW Executive Committee (EXCOM), a body responsible for evaluating EW capabilities and forces.

The US Strategic Command (USSTRATCOM) commander is the operational lead for EMSO under the DoD Unified Command Plan. The Joint Electromagnetic Warfare Center, a subcomponent of USSTRATCOM, is responsible for authoring joint doctrine, such as the recently published Joint Publication 3-85 on joint electromagnetic spectrum operations, and for coordinating with Joint EMSO Cells at combatant commands.[100]

Each service has developed its own organizational approaches for fielding EMSO forces.[101] The US Army combined EW, SIGINT,

Figure 12: Army EWPMT system display

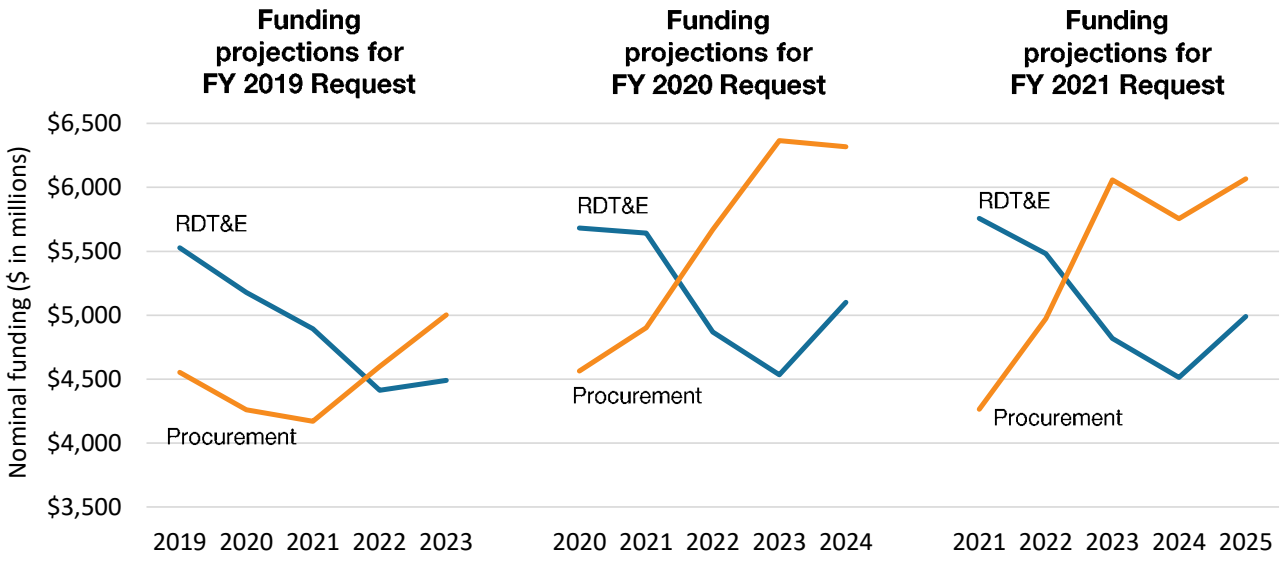
Source: Office of the Director, Operational Test and Evaluation, "Electronic Warfare Planning and Management Tool (EWPMT)," 2019, https://www.dote.osd.mil/Portals/97/pub/reports/FY2019/army/2019ewpmt.pdf?ver=2020-01-30-115324-063.

and cyber personnel and systems under the CEMA construct, with CEMA units incorporated into Brigade Combat Teams and Multi-Domain Task Forces.[102] CEMA units, however, are not incorporated into echelons below the brigade level, which rely on detachments to provide cyber and EW capabilities. The Army has fielded a steadily growing number of man-portable, vehicle-mounted, and unmanned aircraft system (UAS)-equipped CEMA capabilities, including the Electronic Warfare Planning and Management Tool (EWPMT) depicted in figure 12, which allows EW, spectrum management, and cyber operations to be planned, coordinated, and synchronized.[103]

The US Navy organized EMS capabilities under its Information Warfare community. The Navy has fielded the Real-Time Spectrum Operations capability to monitor and deconflict operations in the EMS, and it has enhanced its sailor training through the Center for Information Warfare Training Electromagnetic Warfare Officer Surface Course and the EMSO Certification/Qualification Program. The majority of Navy EMS capabilities are incorporated into maritime and air platforms.

The US Marine Corps has reorganized its EMSO forces into Marine Expeditionary Force Information Groups and established a three-star general as Deputy Commandant for Information. To improve Marines' operational proficiency in EMSO, the Marine Corps established EMSO-specific career paths such as Marine Air-Ground Task Force Electromagnetic Warfare Officer; increased the realism of its training scenarios; and adopted

Figure 13: DoD EW spending trends



Note: FY = fiscal year; RDT&E = research, development, test, and evaluation.

Source: Based on John R. Hoehn, "U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress," Congressional Research Service, April 16, 2020, p. 13, fig. 6.

dedicated opposition forces for live and virtual exercises. Consistent with the Marine Corps' emphasis on distributed and agile operations, most Marine Corps EMS systems are lightweight and either man- or vehicle-portable.

In 2020 the US Air Force combined the 24th Air Force, which specialized in EW operations, with the 25th Air Force, specializing in cyber operations, to form a new 16th Air Force responsible for information warfare. This restructuring builds on efforts in 2019 to establish new squadrons responsible for providing electromagnetic warfare evaluations, cyber assessments, and technical expertise to enable multi-domain mission readiness for combat and mobility air forces.[104] At combatant commands' air operations centers, Air Force personnel staff Non-kinetic Operations Coordination Cells responsible for planning EMS operations and coordinating them with Joint EMSO Cells.[105] Furthermore, within the Department of the Air Force, the nascent Space Force has established a delta (the Space Force equivalent of an Air Force wing) focused on EP and ES for Space Force satellite constellations and ground facilities.

Several major EMSO programs are transitioning from R&D into procurement and fielding, including the SLQ-32 Surface Warfare EW improvement Program Block 2 and 3, F-15 Eagle Passive Active Warning Survivability System (EPAWSS), and EA-18G Next Generation Jammer. As shown in figure 13, DoD spends a relatively constant combined amount on EW RDT&E (research, development, test, and evaluation) and

procurement; therefore, as these large, platform-centric programs enter procurement, they reduce the funding available for RDT&E to develop next-generation EMS technologies. DoD will need more adaptable EMS systems that are decoupled from platforms to reduce the need for these expensive cycles of system recapitalization.

Priorities for Future Development

DoD increasingly views EMS superiority as essential to future warfare, and the EMSO CFT's forthcoming roadmap and implementation plan for the EMS Superiority Strategy will serve as a guide for future EMSO efforts.[106] The focus of this study is technology priorities, but DoD will likely devote significant resources during the next decade to enhancing EMSO professional development and training, including through the fielding of more sophisticated and proliferated virtual and constructive training capabilities.[107]

A few technology areas are likely to be prioritized in DoD EMSO programs, based on the EMS Superiority Strategy and US military services' operational concepts. The level of investment possible in each area, however, will be impacted by the overall budget environment.

- Artificial intelligence and machine learning will be incorporated into nearly all new EMS capabilities. This technology will enable cognitive capabilities across different EMS functions.
- Modular open systems architectures are likely to be increasingly adopted in new manned and unmanned aircraft systems. These architectures may enable improved integration of heterogenous systems and interchangeability in the field.[108]
- Digital modernization will likely remain a top priority for DoD as legacy analog systems are recapitalized.
- Proliferation of 5G may stimulate DoD's adoption of dynamic and automated spectrum sharing and management capabilities.
- EMBM systems are a priority within DoD. The Joint Electromagnetic Warfare Center is developing an EMBM tool that is intended to be used by Joint EMSO Cells in support of combatant commanders (CCDRs) and joint task forces. The Army, Navy, and Marine Corps are continuing to develop their own EMBM systems, although an initiative led by the DoD Chief Information Officer may coordinate if not integrate the different service capabilities.
- Directed energy weapons such as laser and HPM are under development, testing, and fielding by the services. Although the first versions of these systems are reaching US forces, several years of technology maturation will be needed for them to be useful against the most stressing targets, such as cruise missiles.

The US Army and Air Force will likely leverage new rapid acquisition processes in their pursuit of new EMS capabilities, technologies, and systems.[109] For example, in developing the Terrestrial Layer System (TLS) and Multi-Function Electronic Warfare programs, the Army leveraged industry consortia and Other Transaction Authorities (OTA), which are pursuing a family of systems for ground vehicles, large and small UAS, helicopters, and dismounted units.[110] Similarly, the US Air Force ABMS program has assessed EMS systems that can contribute to DoD's JADC2 construct using a series of demonstrations funded through an OTA contract.

The Department of the Navy is using more traditional approaches to pursue upgraded versions of existing EMS systems, most of which are designed to protect platforms. These include block upgrades to the Surface Electronic Warfare Improvement Program for surface combatants and the Integrated Defensive Countermeasures suite for Navy fighter aircraft.[111] Although not devoted only to platform protection, the ALQ-249 Next Generation Jammer program replaces existing ALQ-99 jammers and sequentially fields new EA capabilities through discrete pods focused on the mid, low, and high bands.[112] The Navy is also pursuing a more traditional acquisition approach with

Figure 14: US Space Force Counter Communications System

Source: Space and Missile Systems Center Public Affairs, US Space Force, March 13, 2020, https://www.spaceforce.mil/News/Article/2113447/counter-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/.

new offboard EW systems, including the ALQ-218 Advanced Offboard Electronic Warfare System. The ALQ-218 will initially be carried in a pod by MH-60 helicopters but could be the first of multiple EW systems incorporated into unmanned vehicles.[113]

The Marine Corps is arguably the most advanced of the services in fielding distributed, networked EMS capabilities, organized under its Intrepid Tiger family of systems. Individual Marines' software-defined radios and man-portable EW systems conduct multiple EMSO functions, which can be coordinated and integrated with Intrepid Tiger pods on Marine Corps helicopters and UAVs.[114]

The Space Force is still establishing its R&D and acquisition organizations. However, given the Space Force's doctrinal emphasis on access to and control of the EMS, it will likely prioritize EMS capabilities, including systems like the Counter Communications System (depicted in figure 14) that was transferred to the Space Force from the Air Force.[115]

Summary

The US military's EMSO concepts and capabilities are at an inflection point. DoD recently published a new strategy advocating a more decision-centric approach to EMSO that could afford US forces an advantage against the comprehensive

set of EMS capabilities and organizations deployed by the PRC or Russia. The operational concepts US forces use to guide their organizations and tactics increasingly focus on information as the central competition in warfare. Although doctrine published by the US military services does not yet clarify that their goal is a decision-making, rather than targeting, advantage, the conceptual movement in this direction is already under way.

Slow technology innovation, maturation, and adoption are likely the most significant impediments to US forces regaining EMS superiority. Emerging US military doctrine points toward operational approaches that would circumvent, rather than directly counter, attempts by the PLA or Russian Armed Forces to disrupt US battle networks. The US military services' EMSO capabilities, however, are largely those designed during the later Cold War to protect platforms in confrontations where attrition was the primary mechanism for victory. Upgrades to these legacy EMSO systems consume the bulk of DoD EMSO investment, and may limit the implementation of new concepts that rely on distribution, agility, and maneuver.

New EMS systems that are under development by DoD could better execute the decision-centric approach advanced in the EMS Superiority Strategy. The US military services should accelerate these efforts to implement new ways of achieving and maintaining EMS superiority. In what is expected to be a constrained budget environment, advancing new EMS capabilities will likely require divesting of some legacy EMS systems. The next chapter will describe asymmetries between US, PRC, and Russian EMSO concepts and capabilities; based on this analysis, the final chapter will suggest how DoD should adjust its EMSO technology priorities.

CHAPTER 4. ASYMMETRIES IN ELECTROMAGNETIC SPECTRUM OPERATIONS CONCEPTS AND CAPABILITIES

DoD will need to focus its EMSO development efforts on concepts and capabilities that provide US forces the greatest and most enduring advantages against the PLA and Russian Armed Forces while mitigating US disadvantages. The net assessment methodology offers a way to identify these opportunities by exploiting asymmetries between US and opposing militaries.

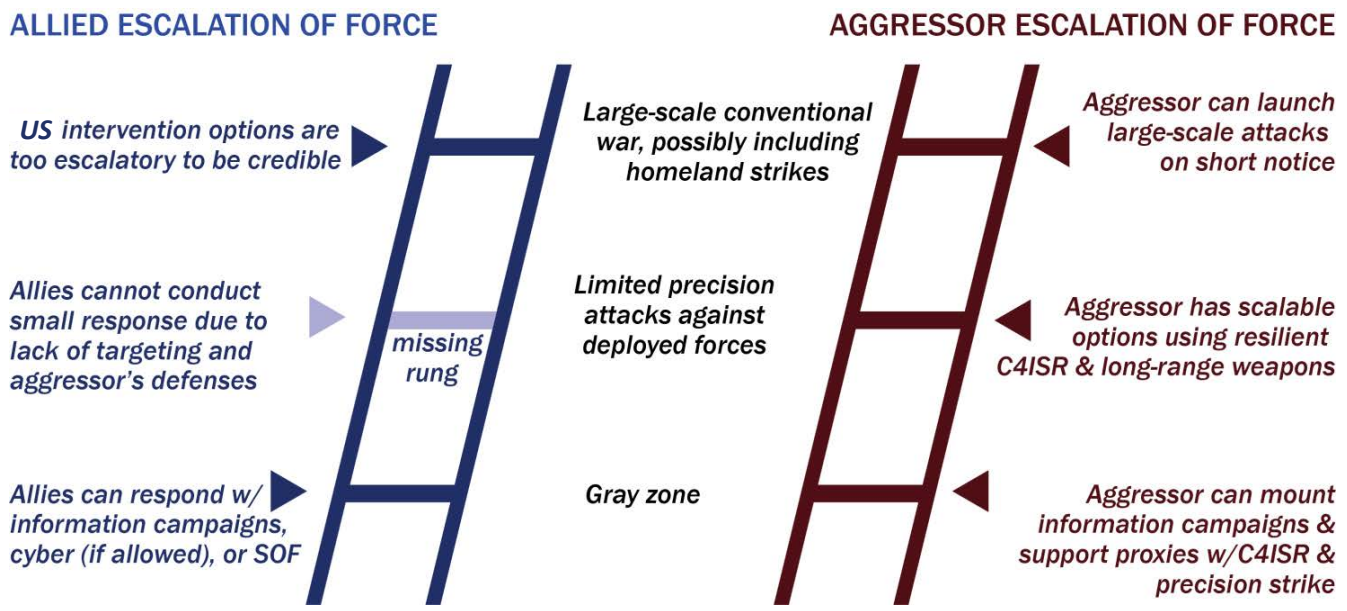
Assessing the strategies, concepts, capabilities, and organizations of the US, PRC, and Russian militaries described in chapters 2 and 3 reveal the following asymmetries that could be leveraged by DoD.

Geography

The PRC and Russian militaries will likely be the home team in future military confrontations given their ongoing gray-zone operations and stated interests in neighboring countries such as

Photo Caption: Polish F-16s escort a B1B Lancer during a training mission for Bomber Task Force Europe, May 29, 2020. Aircrews from the 28th Bomb Wing at Ellsworth Air Force Base, South Dakota, took off on their long-range, long-duration Bomber Task Force mission to conduct interoperability training in the Black Sea region. During the mission, the B-1s conducted training on the Long Range Anti-ship Missile (LRASM). (Photo by Polish Air Force)

Figure 15: Escalation of asymmetry between US forces and aggressor forces based on geographic asymmetries



Note: SOF = special operations forces ; C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

Source: Figure adapted from Bryan Clark and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance*, (Washington, DC: Center for Strategic and Budgetary Assessments, 2017), p. 18.

Taiwan for the PRC and the Baltic countries for Russia. As a result, the PLA and Russian Armed Forces can rely to a greater degree than the expeditionary US military on wired communications and can employ passive and multistatic sensors that require multiple networked arrays and a sophisticated understanding of the regional EM operating environment.

As revisionist powers, the PRC and Russia are also more likely to set the time and place for a confrontation, whereas the US military often must respond to aggression. The resulting proximity of the PLA or Russian Armed Forces to likely areas of conflict enables them to focus military deployments locally and exploit interior lines of support, whereas the US military is distributed globally and depends on extended and vulnerable logistics.

An important escalation asymmetry emerges from the likelihood that the PRC and Russia will have the initiative and be the resident combatant in most potential future confrontations. Both adversaries can base sensors, weapons, and platforms on their home territory while contesting the surface, air, and space for hundreds of miles beyond their borders. US forces will be expeditionary in most conflicts with the PRC and Russia, and therefore will have to operate in international waters and

airspace while carrying their own defenses, and when possible collaborating with allies and partners in the area. As a result, the PLA or Russian Armed Forces can hold US forces at risk and protect PRC or Russian paramilitary and proxy forces in likely areas of conflict, affording the PRC and Russia more rungs on the escalation ladder than the United States (see figure 15). The US military will need to operate in survivable formations that may be disproportionate to the situation or accept the risk that small, proportional force packages will be vulnerable to prompt and devastating attacks.

Technological Innovation

The PLA's concept of system destruction warfare requires development of countermeasures that address specific nodes and vulnerabilities of an opponent's systems of systems. Given the potential targets of PRC aggression, the PLA can plan for the US military being its most likely and significant opponent, whereas the DoD needs to plan for a wide range of potential adversaries. The PLA can also leverage the PRC's robust commercial electronics industrial base to develop new capabilities, enabling it to field a comprehensive and changing collection of EMS systems designed to support its own operations while disrupting those of US forces.

Russia lacks the PRC's military budgets and fusion with civilian industry. Because of these constraints and New Generation Warfare's emphasis on avoiding strengths, the Russian military does not attempt to field new systems that address each new US system or node as the PLA can. Instead, the Russian military tends to incrementally adapt existing EMS systems so it can generally degrade US or NATO power projection while improving the ability of Russian Armed Forces to pursue or support operations consistent with New Generation Warfare.

DoD largely pursues two tracks in new EMS technologies: new capabilities that are designed to support innovative operational concepts, and improvements to existing systems that counter new adversary capabilities. Because new concepts like Joint electromagnetic spectrum operations are not associated with existing major programs, the DoD approach results in the majority of DoD EMSO investment going toward incremental advancements of legacy systems that chase adversary initiatives rather than toward new innovations that create dilemmas for opponents.

Command, Control, and Communications (C3)

The PLA can rely on redundant and resilient communications networks to support a relatively fixed C2 structure of unit commanders, theater commanders, and the Central Military Commission. Furthermore, the proximity and initiative afforded to the PRC as the likely aggressor in a military confrontation with the United States allows it to shape operational scenarios and build plans, branches, and sequels in advance. Although PLA field commanders could improvise during an operation, they may be less inclined to do so given the substantial body of planning and assessment conducted prior to a mission and the reliability of communications with senior commanders.

Although the Russian military is also likely to have proximity and initiative in future confrontations with US or NATO forces, it does not enjoy the PRC's level of communications resilience. Russian Armed Forces therefore are more likely to build initial plans and rely on local commanders to execute them, or to improvise when conditions change, or communications are degraded.

The US military exhibits elements of both the PRC and Russian approaches. With efforts like JADC2 and ABMS, DoD aspires to create the PRC's level of communications reliability so distant commanders at regional headquarters can manage operations across a theater. Under the concept of mission command, US military doctrine directs local commanders to use their initiative and improvise when communications break down. Unfortunately, as noted in chapter 3, DoD has not adequately equipped or prepared US forces for either approach.

Employment of AI

All three competitors considered in this study are aggressively pursuing AI as an element of their overall military force development, but with different priorities for operational systems compared to management and support capabilities. The resulting asymmetry may provide opportunities for US EMS systems development.

PRC officials describe comprehensive adoption of AI by the PLA in command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR) capabilities such as battle management systems, logistics management programs, EMSO and cyber planning tools, EW capabilities, and sensor processing.[116] Although the PLA is also pursuing AI for weapons and unmanned platforms, these weapons and platforms are more accurately described as autonomous. Some, however, have adopted or are adopting AI-enabled capabilities such as automated target recognition.[117]

The Russian military appears to be fielding AI primarily for planning and guiding human-led operations, although other elements of the Russian government and intelligence services employ AI as part of New Generation Warfare cyber operations.[118] The Russian military recently fielded its first EW system described as employing AI to identify targets, choose techniques, assess effectiveness, and respond to an opponent's actions.[119] Experts assess that beyond EMSO, the Russian Armed Forces are beginning to field AI-enabled control systems in autonomous vehicles to improve their ability to avoid threats and reach operational areas to execute pre-planned operations. Like the PLA's, however, these systems may be more accurately described as autonomous.[120]

Until recently, DoD's AI development emphasized its use in operational systems, rather than in planning, analysis, or C2. For example, Project Maven fielded AI-enabled image recognition and intelligence analysis starting during the mid-2010s. Several US communications, EW, and radar systems employ AI to avoid threats and guide EA operations.[121] And weapons such as the Long-Range Anti-ship Missile (LRASM) incorporate AI-enabled algorithms to collaboratively find and engage intended targets.[122] DoD is now expanding its application of AI algorithms to C2 and decision support to commanders as part of programs including ABMS, the US Army's Project Convergence, and the US Navy's Project Overmatch.[123]

EMS Capability Development

As noted above, an asymmetry in technological innovation exists between the PLA's comprehensive systems of systems that target US battle networks, the Russian military's more incremental approach, and DoD's efforts to modernize existing systems while fielding capabilities for disruptive new operational concepts. This asymmetry extends to the EMS as well.

The PLA fields a wide array of EM sensors, communications networks, and EW systems designed to exploit the PRC's position as the home team in potential future conflicts and to target nodes in US military systems of systems. Russian Armed Forces EMS capabilities are more generalized than those of the PLA and do not evolve as quickly to exploit new operational concepts. The sensors, networks, and EW systems fielded by US forces, in contrast, evolve largely in response to improving PLA and Russian military threats, and are only recently incorporating new capabilities to proactively implement new tactics or concepts.

EW and EMSO Organization

Significant asymmetries exist between the DoD and its competitors regarding the organizations that govern and develop EMS capabilities. The PLA developed a unified governance structure for EMS policy in the Joint Staff Department's Network-Electronic Bureau (JSD NEB), which parallels the Russian Armed Forces' EW Commander and staff. The US military, in contrast, divides responsibilities for doctrine and strategy between USSTRATCOM, the EW EXCOM, and the EMSO CFT. Moreover, DoD does not give any of these bodies

the authority to direct EMSO-related spending or acquisition, reducing their ability to implement policy.

The organizational asymmetry extends to EMSO capability development. The PLA and Russian Armed Forces established national-level organizations to develop and field strategic EW capabilities, such as those for disrupting enemy satellite communications, early warning sensors, or C2. The US military has no corollary for the PLA's SSF or the Russian military's Independent EW Brigade, although USSTRATCOM has responsibility for employing wide-area EW systems developed by the US armed services, including the new Space Force. The PRC, Russian, and US militaries are very alike, however, in the development and fielding of operational and tactical-level EMS capabilities by their respective military services.

Deployment of EW Capabilities

Although the PLA, Russian Armed Forces, and DoD all field operational- and tactical-level EMS capabilities through their service branches, the scale and depth of deployment varies significantly. Because of the value they place on EW as an element of their respective military strategies and operational concepts, the PRC and Russian militaries equip units with offensive and defensive EW systems and personnel down to the ground force company, aviation squadron, and naval or paramilitary ship level.

US EW capabilities are deployed to varying echelons of command depending on the service, but generally are held at higher levels of command than in the PLA or Russian Armed Forces. EW systems attached to aviation units or ships are generally focused on defense or self-protection, owing to the position of US forces as the away team in most potential conflicts with the PRC or Russia. Within US ground forces, Marine units down to the company level are being equipped with multifunction EMS systems capable of conducting offensive and defensive EW as part of the Marine Air-Ground Task Force (MAGTF) EW program. Army offensive and defensive EW capabilities such as the Terrestrial Layer System, in contrast, are being fielded at the brigade combat team level and above.[124] And although smaller EW systems—like Tactical Cyber Equipment-C4ISR/EW Modular Open Suite of Standards (CMOSS) Chassis (TCE-CC)—may be detailed to the company and battalion level, they are still attached to brigade combat team, division, and corps-scale formations to enable initial long-range reconnaissance and strike operations.[125]

EMSO Concepts

The US military introduced the EMSO concept to create a coherent framework for EW operations to control the EMS and EMBM to coordinate EMS activities such as EW, sensing, and communications. The Joint EMSO Cells described in Joint Publication 3-85 allow commanders to identify opportunities or challenges emerging from the growing diversity of activities in the EMS. For example, dynamic spectrum management could enable communications, jamming, and sensing to occur on the same frequency at different times; radar or radio signals could be used both to sense and communicate; and EA could interfere with sensing or reveal the location of friendly forces. However, the EMSO concept is relatively new; although it has driven a change in doctrine, the concept has not substantially changed the type of EMS-dependent systems fielded by DoD.

The PRC and Russian militaries do not have publicly released unified concepts for EMS operations, and as described in chapter 2, they largely consider EMS control operations through EW separately from communications and sensing. Within PLA doctrine, the need to coordinate and integrate diverse actions in the EMS is addressed through the systems warfare construct. Each system, such as the reconnaissance-intelligence or command systems, comprises smaller service and unit-level subsystems that are designed to work together in pursuit of operational objectives, including in the EMS.[126] The Russian Armed Forces lack the organizing framework of systems warfare and rely on manual spectrum management and deconfliction to coordinate operations in the EMS.

Summary

The asymmetries between the US, PRC, and Russian militaries provide a basis for assessing how DoD could pursue a more enduring advantage in the EMS. Some asymmetries, such as geography, are difficult to reverse, but could be mitigated or turned into opportunities by changing US military operational concepts and capabilities. Other asymmetries, such as DoD's lead in the EMSO concept and EMBM capabilities, could be expanded, while the lack of distribution in ground force EW systems could be addressed through greater EW capacity.

The next chapter will assess implications of the above asymmetries for DoD EMS technology development and identify ways US forces could accelerate their pursuit of EMS superiority.

CHAPTER 5. TECHNOLOGY PRIORITIES

The asymmetries between US, PRC, and Russian EMSO doctrine, organizations, and capabilities reinforce the value of decision-centric planning and capability development. Differences such as the PRC and Russia's home team advantage and emphasis on well-defined systems of systems create opportunities for the US military to gain an edge through concepts and technologies that increase the number of options available to US forces and improve their adaptability in the move-countermove competition.

Beyond simply pursuing adaptability, however, a fundamental challenge with decision-centric planning is defining the option space in which operations or the development of adaptable capabilities should occur. The opportunities revealed by the net assessment's asymmetries point to the kinds of adaptable technologies DoD should pursue and can be organized into four main categories: capabilities enabling DoD to obviate, rather than overcome, fundamental challenges; capabilities that undermine adversary advantages; capabilities that turn challenges into opportunities; and capabilities that exploit existing US strengths.

The technology priorities encompassed by these categories accept risk because they do not attempt to solve every potential future capability gap. The forecast-centric approach of the Joint Capabilities Integration and Development System (JCIDS), however, is unlikely to succeed within DoD's realistic budget and time constraints and could result in an unfocused set of

Photo Caption: An unmanned aerial vehicle crew with the 82nd Airborne Division's 1st Brigade Combat Team wheels out a Shadow 200 UAV for flight June 7, 2012, at Forward Operating Base Warrior, Ghazni province, Afghanistan. The crew is assigned to Company B, 1st Brigade Special Troops Battalion. (US Army photo by Sgt. Mike Macleod)

technology efforts that are rendered ineffective by the next wave of adversary EMSO innovation. This study recommends that DoD EMS systems efforts prioritize the following areas to establish an enduring advantage within a relevant time and the US military's likely budget constraints.

Capabilities to Obviate, Rather than Overcome, Challenges

The PLA's concept of system destruction warfare uses the PRC's fusion of military and civil R&D sectors to design a comprehensive set of EMS countermeasures that target key US battle network nodes and platforms. Continuing to engage in an extended move-countermove competition with the PLA is costly and time-consuming. For example, expensive platform-based DoD EMSO modernization programs such as the F-15 Eagle EPAWSS, Next Generation Jammer, and Navy SLQ-32 SEWIP are designed in part to overcome adversary threats that will be fielded a decade or more before the new US system is fully deployed. Platform-based systems will also consume a growing fraction of DoD's EMSO-related funding as they transition from development into fielding.[127]

Rather than attempting to directly compete with the PRC's military-industrial complex, the US military should counter PLA system destruction warfare by implementing more adaptive and unpredictable EMS operations enabled by capabilities that are inherently more agile or that can be modified because they are not highly integrated into a monolithic platform. As described below, by creating more options through maneuver in frequency, time, power, and pulse characteristics, US forces could circumvent PLA countermeasures and create new challenges for the PRC military to address.

Capabilities to Undermine Adversary Advantages

The most significant challenges posed by the PLA and Russian Armed Forces derive from geographic asymmetries between the PRC and Russia as resident powers in likely areas of conflict and the United States as an expeditionary power. DoD could overcome some of these challenges by reducing the inherent vulnerabilities created by the US military's current dependence on active sensors like radar, EW systems such as the E/A-18G Growler or TLS that are associated with monolithic platforms or troop formations, and wide-area non-Low Probability of Intercept/Low Probability of Detection (LPI/LPD) communications networks like Link-16 or Common Data Link.

Preventing adversary exploitation of US EMSO systems is an element of EP, which should be given higher priority in US EMSO technology development. The technologies identified below will be critical to enabling this transition in DoD EMSO concepts and tactics.

Passive and multistatic EM sensing

As home teams, the PRC and Russian militaries increasingly rely on passive sensors, multistatic radar, and high frequency/very high frequency (HF/VHF) radar to monitor their air and maritime approaches. Although PLA and Russian Armed Forces sensors are predominantly ground or satellite-based, both militaries are improving the sophistication and networking of their ship- and aircraft-borne active and passive sensors. US forces, as the away team, will need to reduce their EM emissions and signatures across the RF, IR, and visual spectra.

The US military has emphasized signature reduction during the last three decades with stealthy aircraft such as the B-2 Spirit, F-22 Raptor, and F-35 Lightning II or ships like the DDG-51 *Arleigh Burke* and DDG-1000 *Zumwalt*. Although reducing US platform detectability will continue being important, stealth will increasingly be the "table stakes" in military competitions with the PRC or Russia, both of which field low-observable aircraft in their own militaries.[128]

DoD will need to augment stealth with a greater reliance on EO/IR, multistatic, and passive RF sensing to reduce an opponent's

ability to counter-detect and geolocate emissions from manned US units. EO/IR sensors have relatively short ranges compared to passive ELINT and SIGINT detectors, suggesting that US forces should prioritize a shift to RF sensing technologies that do not emit or that use RF sources, such as unmanned vehicles, which are expendable and can be postured away from valuable manned platforms and formations.

Passive and multistatic missile defense

A high priority for passive and multistatic sensing technology development will be missile defense. Current missile defense radars like the Patriot, AN/TPY-2, and SPY-1, -4, and -6 rely on high-power, digital beam steering and multiple beam capabilities to track incoming missiles with the accuracy and precision needed for engagements. These radars are also easily detected and create a counter-targeting risk for missile defense units. Multistatic radar could reduce the risk to receiver sites where surface-to-air missiles could be co-located and could employ attritable or mobile platforms to host the emitter with acceptable risk.

To reduce the vulnerability of missile defense systems, DoD will need to field passive and multistatic sensors that can detect and track subsonic, supersonic, and hypersonic weapons. The emerging generation of anti-ship and land-attack missiles rely less than their predecessors on active RF seekers to lower their likelihood of being counter-detected.[129] In response, US passive air and missile defenses will need to employ IR or EO sensors. The heat signature of fast-moving missiles can often be detected by IR sensors, but only if properly positioned; even with a detection, however, multiple distributed IR sensors are often needed to achieve the precision and responsiveness required for surface-to-air missile engagements.[130] EO sensors offer higher precision than IR sensors, but have relatively shorter range and require cueing because of their relatively small field of view. The precision and coverage afforded by passive sensors could therefore be improved by using multiple, distributed reception arrays.

Networked ES

Passive receiving arrays need to communicate with one another or with multistatic emitters to enable more precise sensing. DoD is using some existing data links, such as Tactical Targeting Network Technology (TTNT), to connect networked receivers, but more secure and less detectable data links will be needed as adversary passive RF sensors improve. Communications management systems could also be used with existing data links to improve their resistance to detection and exploitation by varying signal characteristics to avoid enemy jammers and sensors while supporting friendly operations.

DoD's increased reliance on space-based sensing—through projects such as the Space Development Agency's Hypersonic and Ballistic Tracking Space Sensor or DARPA (Defense Advanced Research Projects Agency) Blackjack program—creates another new opportunity for secure communications.[131] Freed from most atmospheric interference, satellite-based sensors can share data with each other and surface or airborne forces using laser communication systems. Although laser communications will be degraded somewhat when transmitting to the ground or an aircraft, the signal is impacted by the atmosphere only over the last few miles.[132]

Networked EA

US forces will increasingly be constrained in their employment of standoff or modified escort EA from large, manned aircraft or ships due to the range and number of enemy air and surface defenses. For example, although the E/A-18G's new Next Generation Jammer will enjoy increased range, precision, agility, and range of effects compared to its predecessors, the aircraft may be too vulnerable to risk within overlapping missile defense envelopes that can reach more than 200 nautical miles from PRC or Russian territory.[133] As a result, the E/A-18G may be relegated to missions in more permissive environments, such as against naval and ground formations outside of PRC and Russian homeland-based air defenses.

To enable offensive EA operations against capable opponents such as the PLA or Russian Armed Forces, the US military will need to increasingly rely on penetrating escort or stand-in jamming that occurs within range of adversary air or surface defenses.[134] The systems that conduct high-risk EA operations inside these highly-contested areas will need to be expendable or inexpensive enough to be attritable. Creating jamming, decoy, or deception effects using relatively small and cheap unmanned EA platforms will likely require that the EA systems use proximity to the target to make up for their lower power and that they coherently combine their transmissions.

To enable networked EA operations, DoD will need to increase its ongoing efforts to field control systems able to manage multiple unmanned vehicles and their transmitters, as well as the networks able to support the precise timing and low latency required to achieve coherent effects. In parallel, DoD will need to mature unmanned surface and air vehicles that are inexpensive enough to be expendable or attritable, and tamper-protection systems to guard against enemy exploitation when systems are lost.

LPI/LPD active monostatic sensing

As noted above, passive and multistatic sensors generally require multiple distributed arrays to achieve high precision. As an expeditionary force, the US military may have difficulty sustaining multiple sensor systems in position to support missile defense, although this may be possible for protection of specific targets.

In concert with developing improved passive sensing networks, DoD will need to accelerate establishment of LPI/LPD modes for existing radars. For example, active radars could be cued by passive sensors to allow the radar to use a narrow beam that is less vulnerable to counter-detection. Once the target is detected, the radar could then lower its power to the minimum needed given the target's range, and then operate intermittently to track the target, rather than illuminating it continuously. The most extreme form of this approach may be light direction and ranging (LIDAR), which takes advantage of the narrow beams and more precise emissions control possible with lasers.

Multifunction ES and EA capabilities

DoD's increased reliance on distributed passive and multistatic receivers and need for penetrating escort and stand-in EA both suggest the US military should field more smaller, unmanned, and expendable or attritable EMSO platforms. However, DoD cannot afford to employ many specialized EA and ES platforms, even if they are individually less expensive than today's manned multi-mission aircraft, ships, and vehicles. The cost of developing and sustaining separate fleets of jammer, decoy, and sensor platforms may be prohibitive; more importantly, transporting and managing them in theater could be infeasible.

The difficulties involved in using larger numbers of distributed ES and EA vehicles could be alleviated by ensuring that most DoD EW systems are able to perform either sensing or jamming operations, assuming each EW platform already incorporates radios for networked ES and EA. Because the direction of communications will likely differ from the direction needed for sensing or jamming operations, however, multifunctional ES/EA/communications systems may not be a worthwhile investment, especially in small and inexpensive unmanned EW platforms.

Capabilities to Turn Challenges into Opportunities

As noted above, US forces are at a disadvantage against the PLA, which can design comprehensive systems of sensors and EA systems to counter specific US EMS capabilities. The PRC's robust military-civil industrial base could enable rapid execution of a move-countermove cycle in EMS capability development, making DoD efforts to symmetrically gain an advantage expensive and time-consuming. US forces will therefore need to pursue approaches that circumvent the PLA's capability development advantage by adapting in real time using more flexible hardware and AI-enabled software.

AI-enabled, wideband EW and EMS systems

The US military could break out of the EMSO move-countermove cycle by fielding sensor and EW systems that can react to adversary actions in real time and develop and employ new courses of action (COA). This approach could turn the PLA's pursuit of system destruction warfare into a vulnerability, since the capabilities and characteristics of individual PLA systems are relatively fixed. Enabling DoD EMSO this level of flexibility and responsiveness, however, will depend on communications, sensing, and EW systems with wider frequency and dynamic range than most current capabilities, and on control systems that are able to adapt to adversary actions.

To become more adaptive in real-time or between missions, EMS systems will need to derive an increasing portion of their functionality from software, rather than hardware. The software for adaptive jammers, radios, and sensors, however, does not necessarily require deep neural nets or other machine learning–enabled algorithms; it could employ less sophisticated forms of AI such as pre-planned responses, expert systems, or supervised learning. These more explainable forms of AI may be better for EMSO applications because they would be less susceptible to manipulation by opposing cognitive or adaptive EMS systems, which could employ techniques to impart incorrect learning and introduce vulnerabilities into US EMSO control systems.

Automated and AI-enabled reprogramming

Existing EMS capabilities, especially EW systems, are not adaptive, but their software can be revised to recognize new threats, incorporate new techniques, and implement improved decision trees for executing EW operations. Today, this reprogramming effort is time-consuming—both to generate the needed code and to incorporate it into the applicable systems. Automated reprogramming capabilities are widely used in the commercial software industry and are beginning to reach DoD EW maintenance organizations. Accelerating this effort would improve the adaptability of US forces using systems that are not yet able to adapt in real time or to introduce new programs into adaptable systems that are fielded.[135]

Decision support aids and communications management systems

The US military is generally at a C3 disadvantage against adversaries that are the resident power in a conflict. US forces lack the redundant communications and interior lines of support enjoyed by opponents like the PRC or Russian military, which can employ a wide range of ground, air, and space-based jammers to disrupt US forces' communications while sustaining their own networks. Cut off from forces in the field, senior US military leaders would be unable to direct action from distant and well-staffed command centers. Junior leaders delegated command in these cases, however, lack the planning tools or personnel to manage the growing number and diversity of manned and unmanned units under their control.

DoD could turn these C3 challenges into an advantage by giving junior commanders decision support systems to help them develop COAs in the absence of communications with senior leaders and staffs. Several C2 tools are under development that help leaders identify the combinations of sensors and shooters available and in communication, as well as assess the likelihood various COAs will succeed given assumptions about the opponent's capabilities and disposition.[136] With these tools, junior leaders would be able to execute mission command, using their initiative and creativity to fulfill the senior commander's intent. Today, junior leaders executing mission command often must rely on predictable habit or doctrine to formulate COAs on their own. With decision support tools, junior commanders could improvise approaches that will be less predictable for PLA or Russian forces and could create sufficient uncertainty to dissuade further adversary aggression.

Decision support tools should be complemented by communications management systems that identify for commanders which subordinate units are in communication

or that attempt to establish communications with forces the commander needs to execute desired COAs.[137] Communications management would help avoid a unit in communication with multiple commanders from being "double tapped" and, more importantly, allow US forces to minimize their counter-detection risk by sustaining the lowest-bandwidth and least-continuous communications that are consistent with the commander's intent and orders.

Capabilities to Exploit Existing US Strengths

Although DoD has fallen behind in some key aspects of the move-countermove competition with the PLA and Russian Armed Forces, there are some areas in which DoD has an edge. The US military should build on these advantages to create challenges for the PRC and Russia and compel them to keep pace with US developments. As part of DoD's overall technology strategy, exploiting these areas of advantage can reduce the resources opposing countries can devote to expanding their own areas of superiority.

Virtual and constructive EW/EMSO environments

As noted in chapter 3, DoD needs to improve its ability to conduct virtual and constructive EMSO training and concept development. Live, virtual, and constructive (LVC) approaches could improve the quality of home station training, expand the range of tactics US forces could practice, and reduce the vulnerability of US training operations to adversary surveillance and exploitation.

The US military could exploit its nascent investments in LVC-based EMSO experimentation and training by accelerating the introduction of virtual and constructive tools and environments at each organizational level. Even unsophisticated tools for individual units at home station would allow a dramatic improvement in proficiency and readiness for challenging training and certification events at Combat Training Centers. And establishing more comprehensive national networks for virtual and constructive training would allow faster concept innovation and evaluation, as well as incorporation of tactics and technologies described above that are essential to restoring the US EMS advantage.

AI-enabled EMBM

The US military could capitalize on the lack of EMSO concepts and doctrine in the PLA and Russian Armed Forces and exploit the emerging generation of more adaptable EMS capabilities by accelerating the fielding of operationally useful EMBM systems. AI-enabled algorithms offer the potential for faster and more adaptable EMBM systems; but initial EMBM capabilities like the US Army EWPMT program, which use traditional models to support more dynamic spectrum management, visualization, and pre-planned responses, would still substantially improve the ability of US forces to operate in the EMS. AI-enabled models should be incorporated into EMBM systems as they are refined.

Open architecture hardware standards

Modularity is an essential element of improving system hardware adaptation. The PLA's diversity of EW systems could create an integration challenge when introducing new hardware and increase sustainment cost and complexity. The US military has an advantage in its use of open architecture in mission systems using standards such as DoD's Sensor Open Systems Architecture (SOSA), Modular Open Standards Approach (MOSA), the Navy's Future Airborne Capability Environment (FACE), the Air Force's Open Mission System (OMS) framework, or the US Army's Vehicle Integration for C4ISR/EW Interoperability (VICTORY).[138]

Increased adoption of open architectures in US military platforms and vehicles would allow use of more modular EMS systems that could be more easily exchanged and modified. This shift would allow DoD to speed up technological innovation and enable the development and implementation of new operational concepts that exploit new EMS systems.

Open architecture software tools

Another approach to open architecture is interoperability between systems. Composing networked EA and ES systems of systems will depend on having common communication standards. The diversity of PLA EW systems will constrain the composability of PLA forces; similarly, the proliferation of DoD data standards limits the variety of systems that can be employed for EMSO. New interoperability toolkits like the System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) use graphing techniques like Google's search algorithm to build software interfaces on demand that allow disparate networks to talk to one another.[139]

Summary

DoD is pursuing the technologies needed to improve US forces' ability to operate at acceptable risk in highly contested areas and gain an advantage in EMS move-countermove competitions with great power adversaries. These efforts, however, receive less prioritization and funding than activities associated with recapitalizing platform-based EW systems that support legacy operational concepts.

The US military will need to more aggressively pursue new EMS technologies that address the fundamental challenges and opportunities facing US forces. By adapting more passive and multistatic sensing, US forces will improve their ability to defend themselves and target the enemy on contested areas.

More importantly, DoD's position in the EMSO move-countermove competition will be improved through a system of systems approach—one that is enabled by networked EA and ES, EMBM, and open architecture systems and software, and that combines more adaptable EMS capabilities (made possible with software reprogramming), wideband antennas and processors, and virtual and constructive training environments. DoD should prioritize these technologies and accept risk in legacy systems focused on platform self-protection or infeasible concepts such as standoff escort jamming.

CHAPTER 6. CONCLUSION

The US military is at an EMS disadvantage compared to its great power competitors. This situation is largely the result of two decades of neglect following the end of the Cold War and a continued emphasis on forecast-centric planning in its capability development. Although DoD raised its spending and leadership focus on communications, sensing, spectrum management, and EW during the 2010s, these efforts were not aligned to support a coherent concept and strategy for regaining EMS superiority. As a result, the US military devoted significant resources to modernizing a small number of platform-centric legacy EMS systems and failed to field new technologies and associated operational concepts that could give US forces an advantage in future EMS move-countermove innovation cycles.

DoD is at a crossroads today in terms of EMS-related technology development. The 2020 EMS Superiority Strategy and operational concepts for EMSO and EMBM advance new approaches to regain EMS advantage by improving the adaptability of US EMS capabilities both during and between operations. The resulting expansion of options for commanders and leaders would allow US forces to break out of today's move-countermove cycle in EMS innovation.

Adaptability alone, however, will not be enough to gain and sustain EMS superiority against capable opponents like the PRC and Russia that can focus their capability development against the US military. DoD will need to prioritize adaptable technologies that exploit asymmetries between US and

Photo Caption: The sun rises above Camp Taji, Iraq, silhouetting the MQ-1C Gray Eagle, Nov. 21 2020. The aircraft is being tested by QRC1-R1, a specially trained drone unit attached to the Enhanced Combat Aviation Brigade, 1st Infantry Division. (US Army photo by Spc. Roland Hale)

adversary forces to obviate, rather than overcome, fundamental challenges, undermine adversary advantages, turn challenges into opportunities, and exploit US strengths.

Technology priorities such as EP capabilities for passive and multi-static sensing, distributed and networked EA, or AI-enabled EMBM and reprogramming will require accepting risk in traditional approaches to EMS missions. But the US military lacks the time and resources to gain a lead in EMSO against PRC and Russian forces using a symmetric system versus system competition. By the time DoD catches up, the PLA or Russian Armed Forces could exploit their EMS superiority to support aggression against their neighbors. DoD's choice is whether to accept continued erosion of its edge in the EMS or to make bold bets on the technologies most likely to circumvent or reverse the inherent advantages enjoyed by its great power competitors.

The technology priorities described in this report represent the US military's best opportunity to establish enduring EMS superiority. They are all being pursued by DoD to varying degrees, but most are merely being sustained rather than accelerated in support of a new approach to EMSO. To reverse trends of the last three decades and give the PRC and Russia challenges to address, funding and attention will need to shift to these new priorities and away from legacy programs that helped US forces win conflicts since the Cold War.

GLOSSARY OF TERMS AND ACRONYMS

ABMS Advanced Battle Management System

AI artificial intelligence

C2 command and control

C3 command, control, and communications

C3ISR command, control, communications, intelligence, surveillance, and reconnaissance

C4 Command, Control, Communications, and Computers

C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CEMA cyber electromagnetic activities

CFT Cross-Functional Team

COA course of action

CSBA Center for Strategic and Budgetary Assessments

DoD Department of Defense

EA electronic attack

ELINT electronic intelligence

EM electromagnetic

EMBM electromagnetic battle management

EMS electromagnetic spectrum

EMSO electromagnetic spectrum operations

EMW Electromagnetic Maneuver Warfare

EO/IR electro-optical/infrared

EP electronic protection

EPAWSS Eagle Passive Active Warning Survivability System

ES electronic support

EW electronic warfare

EW EXCOM EW Executive Committee

EWPMT Electronic Warfare Planning and Management Tool

HPM high-power microwave

IR infrared

ISR intelligence, surveillance, and reconnaissance

JADC2 Joint All Domain Command and Control

KTK Comprehensive Technical Control

LPD Low Probability of Detection

LPI Low Probability of Intercept

LVC live, virtual, and constructive

NDS National Defense Strategy

OTA Other Transaction Authorities

PAFMM People's Armed Forces Maritime Militia

PLA People's Liberation Army

PRC People's Republic of China

RDT&E research, development, test, and evaluation

RF radiofrequency

SIGINT signals intelligence

SSF Strategic Support Force

TLS Terrestrial Layer System

UAS unmanned aircraft system

UAV unmanned aerial vehicle

USSTRATCOM US Strategic Command

VCJCS Vice Chairman of the Joint Chiefs of Staff

ENDNOTES

1 Congressional Budget Office, "An Update to the Budget Outlook: 2020 to 2030."

2 US Joint Staff, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)."

3 This analysis comes from John Stillion and Bryan Clark, *What It Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: CSBA, 2015), https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions.

4 US Department of Defense, "2020 Department of Defense Electromagnetic Spectrum Superiority Strategy."

5 See, for example, Roche and Mahnken, "What Is Net Assessment?"; Cohen, "Net Assessment: An American Approach"; Pickett, Roche, and Watts, "Net Assessment: A Historical Review"; Rosen, "Net Assessment as an Analytical Concept"; and Bracken, "Net Assessment: A Practical Guide."

6 DoD recently revised its doctrine to subsume electronic warfare into the broader category of EMSO. EMSO actions exploit, attack, protect, and manage the EMS and rely on personnel and systems from EW, EMS management, intelligence, space, and cyberspace mission areas. US Joint Staff, "Joint Publication 3-85: Joint Electromagnetic Spectrum Operations," May 22, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

7 H. H. Gaffney, "Capabilities-Based Planning in the Coming Global Security Environment," Center for Naval Analysis, Alexandria, VA, 2004, https://www.cna.org/CNA_files/PDF/D0010880.A1.pdf.

8 The most significant recent authoritative EW studies include the following: Defense Science Board (DSB), *21st Century Military Operations in a Complex Electromagnetic Environment* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2015), https://apps.dtic.mil/dtic/tr/fulltext/u2/1001629.pdf; Government Accountability Office, *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight* (Washington, DC: US Library of Congress, 2012), https://www.gao.gov/assets/600/592211.pdf; Madison Creery, "The Russian Edge in Electronic Warfare," Georgetown Security Studies Review, June 26, 2019, https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/; and Robert O. Work and Greg Grant, *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics* (Washington, DC: Center for a New American Security, 2019), especially p. 7, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf?mtime=20190531090041.

9 Jeff Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

10 Chinese military literature suggests that there are four target types that PLA planners seek when attempting to paralyze the enemy's operational system: strikes that degrade or disrupt the flow of information within the adversary's operational system; strikes that degrade or disrupt that operational system's essential nodes, which include, but are not limited to, its C2, reconnaissance intelligence, and firepower capabilities; strikes that degrade or disrupt the architecture of the adversary's operational system, which includes the physical nodes of the previously mentioned capabilities and therefore would encompass (for example) the entire C2 network, reconnaissance intelligence network, or firepower network; and strikes that disrupt the time sequence and/or tempo of the enemy's operational architecture, which serves to degrade and ultimately undermine the operational system's own "reconnaissance control-attack-evaluation" process. Engstrom, *Systems Confrontation and System Destruction Warfare*, p. xi.

11 Zi Yang, "PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of 'The Winning Mechanisms of Electronic Countermeasures,'" *China Brief* 19, no. 3 (2019), https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/.

12 J. Michael Dahm, "China: Electronic Warfare," presentation at Hudson Institute EW & EMSO Workshop, July 15, 2020. A corollary concept is "information blockade," or the ability to control the information environment and deny information to adversaries. See US Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," 2020, p. 74, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-dod-china-military-power-report-final.pdf.

13 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: Institute for National Strategic Studies, 2018), p. 15, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

14 Zi Yang, "Blinding the Enemy: How the PRC Prepares for Radio Countermeasures," *China Brief* 18, no. 6 (2018), https://jamestown.org/program/blinding-the-enemy-how-the-prc-prepares-for-radar-countermeasures/.

15 US Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," pp. 51, 63–64.

16 For more information on the PLA's electromagnetic spectrum management systems, please see the following: China Military Online, "Training for PLA Electromagnetic Spectrum Management Troops Held," October 15, 2013, http://en.people.cn/90786/8426593.html; John Dotson, "Military-Civil Fusion and Electromagnetic Spectrum Management in the PLA," Jamestown Foundation, October 8, 2019, https://jamestown.org/program/military-civil-fusion-and-electromagnetic-spectrum-management-in-the-pla; Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy: A View from Chinese Strategists* (Montgomery, AL: China Aerospace Studies Institute, 2020), p. 55, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/CASI_China_Military_Civil_Fusion_Strategy.pdf; and 数字冰雹信息技术 [Digital Hail Information Technology], https://www.digihail.com/case/casehtjg.html.

17 Cited in Leng Feng, *Toward the Transformation of PLA Military Training under Conditions of Informationization* (Stockholm: Institute for Security and Development Policy, 2014), p. 23.

18 Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2019: Annual Report to Congress," 2019, p. ii, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

19 Ibid, pp. 22, 48–49.

20 US Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," pp. 68, 82–83.

21 For additional information on this subject, please see J. Michael Dahm, "A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea: Electronic Warfare and Signals Intelligence," South China Sea Military Capabilities Series, Johns Hopkins Applied Physics Laboratory, 2020, https://www.jhuapl.edu/Content/documents/ewandsigint.pdf. Peter Dutton has also pointed out the employment of EW systems by PAFMM (People's Armed Forces Maritime Militia) vessels. PAFMM's passive EMS-related operational methods include use of corner reflectors, steaming in formation, "floated" chaff cannisters, smoke cover, false heat sources, and militia vessels protected by "electromagnetic attenuation and absorption technologies." PAFMM's active EMS-related measures and operations include the use of special warfare militia detachments, electronic jamming, false radio emissions and "baiting," creation of false signals (for ships, missiles, and aircraft), and acting as an opposition force for training PLAN units. Peter Dutton, "China Gray Zone Operations and EW/EMSO," presentation at Hudson Institute EW and EMSO Workshop, July 30, 2020. For information on PLA use of laser systems in Djibouti, please see Aaron Mehta, "Two US Airmen Injured by Chinese Lasers in Djibouti, DoD Says," *Defense News*, May 3, 2018, https://www.defensenews.com/air/2018/05/03/two-us-airmen-injured-by-chinese-lasers-in-djibouti/.

22 Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," p. 141.

23 Ibid., p. 162.

24 US Department of State, "Military-Civil Fusion and the People's Republic of China," https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

25 For information on China's 5G advantages and opportunities to enhance US and allied 5G competitiveness, please see Bryan Clark and Daniel Patt, "Weaponizing the 5G Value Chain: A Two-Pronged Strategy to Establish America's Lead in Next-Generation Telecommunications," Hudson Institute, September 2020.

26 Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, "Evaluating Global Exposure to China's Defense-Industrial Base," C4ADS, 2019, pp. 51–53, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d95fb48a0bfc672d825e346/1570110297719/Open+Arms.pdf.

27 Jiang Jie, "Private Companies Hope for Relaxed Requirements in Military-Civilian Integration," People's Daily Online, April 13, 2017, http://en.people.cn/n3/2017/0413/c90000-9202603.html; 张达 [Zhang Da], "专注大屏可视化决策系统，「数字冰雹」深耕航天军工、智慧城市与网络安全" [With a focus on large-screen visualized decision-making systems, 'Digital Hail' deeply cultivates aerospace military industry, smart city, and network security sectors], 36kr, November 24, 2017, https://36kr.com/p/1722020855809.

28 US Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," p. 141.

29 For additional information on Russian EW, see Jonas Kjellén, "Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces," Swedish Ministry of Defence, 2018, https://www.foi.se/rest-api/report/FOI-R--4625--SE; and Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, Estonia: International Centre for Defence and Security, 2017), https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

30 Glen E. Howard and Matthew Czekaj, eds., *Russia's Military Strategy and Doctrine* (Washington, DC: Jamestown Foundation, 2019), pp. 164–76, https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web-1.pdf?x30147.

31 Valeriy Gerasimov, "Tsennost' nauki v predvidenii," *Voyenno Promyshlennyy Kuryer*, February 26, 2013, https://vpk-news.ru/articles/14632.

32 Howard and Czekaj, eds., *Russia's Military Strategy and Doctrine*, p. 168.

33 Ibid., pp. 308–09.

34 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 2.

35 JB Vowell, "Maskirovka: From Russia, with Deception," RealClearDefense, October 10, 2016, https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html.

36 Technical advances in RF-enabled cyber capabilities, and recognition of the utility of close integration of these capabilities, may prompt Russia to integrate them further.

37 These four concepts supersede two earlier concepts: radio-electronic informational blockade and radio-electronic strike. Michael Kofman, "Russian EW Strategy and Concepts," presentation at Hudson Institute EMS Workshop on US and Adversary Concepts, July 24, 2020.

38 Kjellén, "Russian Electronic Warfare," pp. 29–30.

39 Looking toward the future, Roger N. McDermott (*Russia's Electronic Warfare Capabilities to 2025*, p. 10) has postulated that "with greater state funding, by 2025 or later, the Electronic

Warfare Force could emerge as a new combat arm," as "Russia's military theorists recognize the EMS as another legitimate domain of warfare, in addition to land, air, sea and space." The establishment of the Electronic Warfare Situational Center and the Unified Information Space of the Russian Armed Forces may over time support advocates who propose the creation of an Electronic Warfare Force combat arm, or an Information Warfare combat arm, which would conduct operations across the information-technological and information-psychological spheres.

40 Kjellén, "Russian Electronic Warfare," pp. 31–32.

41 The largest and most capable EW units are the Ground Forces' EW brigades. Every one of the Ground Forces' four brigades has four EW battalions and one company. These brigades are responsible for providing combat support to maneuver brigades and are equipped with long-range systems, such as the Murmansk-BN, Krasukha, and Moskva systems, as well as numerous medium- and short-range systems. Other smaller battalions, companies, detachments, and units provide EW capabilities throughout the service branches and independent combat arms, with EW units paired directly with other units. Moreover, the organization of EW forces can be scaled to suit operational demands. Russia may stand up more EW brigades in the future. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 6.

42 Kjellén, "Russian Electronic Warfare," pp. 33–34.

43 Russian Defense Policy, "Electronic Warfare Chief Interviewed," May 30, 2017, https://russiandefpolicy.com/tag/yuriy-lastochkin/.

44 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 15.

45 Ibid.

46 Ibid.

47 Ibid., pp. 15–16.

48 Samuel Bendett, "Use of Electronic Warfare on Russian UAV Platforms," Center for Naval Analysis, June 2017.

49 Bruce Jones, "Russia's Northern Fleet First to Receive Newest EW Systems," *Jane's Defence Weekly*, April 18, 2017, https://janes.ihs.com/Janes/Display/jdw65385-jdw-2017.

50 Ibid.

51 This mobility enables Russian EW forces to operate in proximity to other Russian forces and facilitates their execution of passive defense measures, such as tactical mobility and camouflage, concealment, and deception.

52 A family of EW capabilities ensures Russian EW units can provide appropriate effects at any scale of operation. Russian EW supports mobile units such as maneuver forces, fires, and air and missile forces. EW units also protect fixed critical assets, such as air and naval bases, command and control nodes, and critical infrastructure. Although Russian forces are improving their C2 of EW with other units (such as air defense troops) and value EMBM, they are trained to fight with degraded communications capabilities and have numerous redundant communications systems, including homeland-based wired networks. Given their training and redundancies, Russian EW units expect and would likely be able to operate in a mutually denied EMS environment.

53 The inclusion of directed energy systems in the EW force recognizes the utility of systems operating in different wavelengths and power levels for different missions. It is also worth noting that multispectral camouflage systems, obscurants, counter-EO/IR systems, and physical and electronic decoys are proliferated throughout the Russian armed forces, especially in air and missile defense and offensive fires units.

54 Leveraging new computing capabilities, EW systems are reducing the amount of human operator input required to execute operations, which reduces risk to human operators—especially when operating active transmitters. The use of automation is also accelerating Russian forces' ability to assess the EMS and implement distributing sensing and attack operations. These new capabilities also facilitate a shift away from continuous, high-power jamming to lower-power jamming that employs more spoofing and other deceptive measures.

55 Howard and Czekaj, eds., *Russia's Military Strategy and Doctrine*, p. 46.

56 Organization for Security and Co-operation in Europe, "Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 10 August 2018," August 14, 2018, https://www.osce.org/special-monitoring-mission-to-ukraine/390236; McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 21. Although separate from the Russian EW organizational structure, Russia and Belarus have a unified EW system in which information from each country's systems in that operating area are passed to the other. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 6.

57 Kjellén, "Russian Electronic Warfare," p. 35.

58 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 8.

59 Konrad Muzyka and Mark Galeotti, "Zapad Exercises Underline Russia's Domestic Security Concerns," *Jane's Intelligence Review*, October 31, 2017, https://janes.ihs.com/Janes/Display/FG_671883-JIR; Samuel Cranny-Evans, "Russia Trials New EW Tactics," *Jane's Defence Weekly*, June 14, 2019, https://janes.ihs.com/Janes/Display/FG_2095796-JDW.

60 Samuel Cranny-Evans, Mark Cazalet, and Christopher F. Foss, "The Czar of Battle: Russian Artillery Use in Ukraine Portends Advances," *Jane's International Defence Review*, April 24, 2018, https://janes.ihs.com/Janes/Display/FG_901376-IDR.

61 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 25.

62 Ibid.

63 Ibid., p. 22.

64 Ibid., pp. iv–v.

65 The Electronic Warfare Force has a rigorous education program for professional EW soldiers, which aims to displace a past heavy reliance

on conscript servicemen. Although this program ensures the development of highly proficient operators who are technically knowledgeable in how to use their own systems and can innovate new approaches, it has slowed the ability of the force to fill EW billets. Accordingly, a continued priority will be the training of soldiers, prioritizing quality over quantity. Timothy Thomas, *Russian Military Strategy: Impacting 21st Century Reform and Geopolitics* (Foreign Military Studies Office, 2016), p. 156.

66 The Russian Armed Forces have sought to maximize lessons learned from large-scale exercises such as Electron 2016, and have also allowed EW operators to gain experience by rotating them into combat operations in Ukraine and Syria. Moreover, Russian EW forces are increasing the amount of virtual and constructive training, which allows operators to employ the full range of their systems' capabilities with reduced risk of adversary intelligence collection.

67 This center will be a subordinate component of the Unified Information Space of the Russian Armed Forces and will aim to provide an organization and system of systems capable of assessing and fusing information from the information-technological and information-psychological spheres. Howard and Czekaj, eds., *Russia's Military Strategy and Doctrine*, pp. 53–54.

68 Russian Defense Policy, "Electronic Warfare Chief Interviewed," May 30, 2017, https://russiandefpolicy.com/2017/05/30/electronic-warfare-chief-interviewed-2/.

69 For a discussion of explosive-driven HPM systems, please see A. Neuber, A. Young, M. Elsayed, J. Dickens, M. Giesselmann, and M. Kristiansen, "Compact High Power Microwave Generation," 2008, https://www.semanticscholar.org/paper/Compact-High-Power-Microwave-Generation-Neuber-Young/46bf1c5b94956a973bdf102c853893f2b910f3f6?p2df.

70 These techniques would include both traditional EW and cyber techniques, possibly operating together.

71 In part, this priority reflects a desire to shift to new lower-power and harder to locate EW capabilities, as opposed to a traditional Russian reliance on high-powered jammers.

72 Systemology enabled by cognitive or artificial intelligence systems has been a significant area of interest for Russian EW forces and the Russian military in general. In a clarion call that has echoed throughout the EW enterprise, Russian dictator President Vladimir Putin asserted in 2017 that "whoever becomes the leader in this sphere will become the ruler of the world." RT, "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day," September 1, 2017, https://www.rt.com/news/401731-ai-rule-world-putin.

73 TASS, "Russia to Develop Advanced Radio-photonic Radars for 6th-Generation Fighter Jets," July 9, 2018, https://tass.com/defense/1012445.

74 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 10.

75 In the past, Russia collaborated with close allies on EW. For example, in 2007 a Russo-Belarus cooperative effort developed a new EW upgrade for the MiG-29 and Su-27/30 aircraft. More recently, however, Russian EW development has been domestically focused. Reuben F. Johnson, "BARP Exhibits New Satellite EW System," *Jane's International Defence Review*, September 10, 2007, https://janes.ihs.com/Janes/Display/idr10833-idr-2007.

76 Sergey Sukhankin, "Russian Capabilities in Electronic Warfare: Plans, Achievements and Expectations," RealClearDefense, July 20, 2017, https://www.realcleardefense.com/articles/2017/07/20/russian_capabilities_in_electronic_warfare_111852.html.

77 Another important EW company is STT, which designs and manufactures UAVs, some of which perform EW functions.

78 McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 17.

79 According to Major General Lastochkyn, international sanctions and Ukraine-related challenges have "mostly been overcome, although some problems do exist." Cited in Sukhankin, "Russian Capabilities in Electronic Warfare."

80 Defense Science Board (DSB), *21st Century Military Operations in a Complex Electromagnetic Environment*; Government Accountability Office, *Electronic Warfare: DOD Actions Needed*; Creery, "The Russian Edge in Electronic Warfare"; and Work and Grant, "Beating the Americans at their Own Game," especially p. 7.

81 John Hoehn, "U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress," Congressional Research Service, April 16, 2020, https://fas.org/sgp/crs/natsec/R45756.pdf; US Department of Defense, Electromagnetic Spectrum Operations Cross-Functional team (EMSO CFT), "Studies and References," https://emso.defense.gov/Background/Studies-References/.

82 James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), p. 5.

83 Theresa Hitchens, "Exclusive: J6 Says CJADC2 Is A Strategy; Service Posture Reviews Coming," *Breaking Defense,* January 4, 2020, https://breakingdefense.com/2021/01/exclusive-j6-says-CJADC2-is-a-strategy-service-posture-reviews-coming/.

84 David Larter, "US Navy, Air Force team up on new 'Manhattan Project'," December 4, 2019, C4ISRNet, https://www.c4isrnet.com/naval/2019/12/06/us-navy-air-force-team-up-on-new-manhattan-project/; Jen Judson and Nathan Stoudt, "At Project Convergence, the US Army experienced success and failure — and it's happy about both," Defense News, October 12, 2020, https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergence-the-us-army-experienced-success-and-failure-and-its-happy-about-both/; Eric A. McCoy, "Sustainment Revolution | Implications of Artificial Intelligence for Army Sustainment," Army Sustainment, July 22, 2020, https://www.army.mil/article/237343/sustainment_revolution_implications_of_artificial_intelligence_for_army_sustainment; Charles Pops, "Advanced

Battle Management System field test brings Joint Force together across all domains during second onramp," US Air Force, September 3, 2020, https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across/.

85 The projected future EMOE is described in US DoD, "DoD EMS Superiority Strategy," (Washington, DC: DoD, October 2020), https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

86 Theresa Hitchens, "ABMS Demo Proves AI Chops For C2," *Breaking Defense*, September 3, 2020, https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

87 US Department of Defense, "2020 Department of Defense Electromagnetic Spectrum Superiority Strategy." In parallel, the EMSO Cross-Functional Team has started writing a Roadmap and Implementation Plan to achieve the five goals outlined in the strategy.

88 US Joint Staff, "Joint Publication 3-85: Joint Electromagnetic Spectrum Operations."

89 Ibid., p. i.

90 The Army and Navy treat EMSO as an aspect of "Information Warfare," the Air Force as an aspect of "Information Operations," and the Marine Corps as an aspect of the "Information Environment." A concern among some in the EMS community is that this approach may undervalue the importance of EMS capabilities.

91 US Army, "TRADOC Pamphlet 525-3-1: The US Army in Multi-Domain Operations 2028," US Army Training and Doctrine Command, December 6, 2018, https://www.hsdl.org/?view&did=820569.

92 Steven Stover, "Army Developing Expeditionary Cyber-electromagnetic Teams to Support Tactical Commanders," US Army, February 8, 2018, https://www.army.mil/article/200262/army_developing_expeditionary_cyber_electromagnetic_teams_to_support_tactical_commanders#:~:text=CEMA%20is%20an%20Army%20initiative,and%20Information%20Operations%20support%2Feffects.

93 US Army, "TRADOC Pamphlet 525-8-6: The US Army Concept for Cyberspace and Electronic Warfare Operations," US Army Training and Doctrine Command, January 2018, https://fas.org/irp/doddir/army/tp525-8-6.pdf.

94 US Navy, "CNO Visits Navy Warfare Development Command," April 13, 2017, https://www.navy.mil/submit/display.asp?story_id=99893.

95 John Joyce, "Navy Expands Electromagnetic Maneuver Warfare for 'Victory at Sea,'" Navy News Service, November 2, 2017. Guides and manuals include the Surface Electronic Warfare Guide, the TACMEMO 3-51.1-15, EMSO Afloat, and the NTTP 3-13.2 IWC Manual.

96 David H. Berger, "Commandant's Planning Guidance: 38th Commandant of the Marine Corps," US Marine Corps, 2019, p. 11, https://www.hqmc.marines.mil/Portals/142/Docs/%2038th%20Commandant%27s%20Planning%20Guidance_2019.pdf?ver=2019-07-16-200152-700.

97 US Air Force, "Annex 3-1: Department of the Air Force Role in Joint All-Domain Operations," 2020, p. 3, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-1/Annex-3-1-DAF-Role-in-JADO.pdf.

98 US Air Force, "Annex 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations," 2019, https://www.doctrine.af.mil/Operational-Level-Doctrine/Annex-3-51-EW-and-EMS-Ops/.

99 US Space Force, "Spacepower: Doctrine for Space Forces," June 2020, pp. xiii, 25–26, 51, https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

100 The Joint Electronic Warfare Center is also responsible for coordinating and when possible integrating US operations with allies and partners.

101 For example, the Army and Marines have three-star generals leading their EMSO initiatives; the Navy has a two-star admiral; and the Air Force has a one-star general.

102 US Army, "Army Field Manual 3-12: Cyberspace and Electronic Warfare Operations," April 11, 2017, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf.

103 US Army, "Electronic Warfare Planning and Management Tool," US Army, https://asc.army.mil/web/portfolio-item/iews-electronic-warfare-planning-and-management-tool-ewpmt/.

104 Air Combat Command, "87th Electronic Warfare Squadron Activated," May 17, 2019, https://www.acc.af.mil/News/Article-Display/Article/1850986/87th-electronic-warfare-squadron-activated/.

105 US Air Force, "Annex 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations."

106 DoD's focus on the EMS has in part been stimulated by congressional oversight and direction to conduct multiple EMSO assessments.

107 For more information on live, virtual, and constructive training, please see Bryan Clark, Whitney Morgan McNamara, and Timothy A. Walton, *Winning the Invisible War: Gaining an Enduring US Advantage in the Electromagnetic Spectrum* (Washington, DC: Center for Strategic and Budgetary Assessments, 2019), pp. 24–25, 52–53, https://csbaonline.org/uploads/documents/Winning_the_Invisible_War_WEB.pdf.

108 Another benefit of this approach is that it may reduce the likelihood of "vendor lock," in which particular system vendors exercise control over the development or maintenance of those systems.

109 Charles Pope, "Advanced Battle Management System Field Test Brings Joint Force Together across All Domains During Second Onramp," US Air Force, September 3, 2020, https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across/.

110 Mark Pomerleau, "Here's What the Army Is Looking for in Its New EW Program," C4ISRNet, February 21, 2019, https://www.c4isrnet.com/electronic-warfare/2019/02/21/heres-what-the-army-is-looking-for-in-its-new-ew-program/; Mark Pomerleau, "Army Plans to Award Major EW-Drone Contract This Year," C4ISRNet, March 2, 2018, https://www.c4isrnet.com/electronic-warfare/2018/03/02/army-plans-to-award-major-ew-drone-contract-this-year/.

111 US Navy, "Surface Electronic Warfare Improvement Program," April 28, 2020, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167559/surface-electronic-warfare-improvement-program-sewip/; US Naval Air Systems Command, "Integrated Defensive Electronic Countermeasures," https://www.navair.navy.mil/product/Integrated-Defensive-Electronic-Countermeasures-IDECM.

112 US Naval Air Systems Command, "Next Generation Jammer," https://www.navair.navy.mil/product/Next-Generation-Jammer.

113 Lockheed Martin, "Advanced Off-Board Electronic Warfare (AOEW)," https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare/surface-ew.html.

114 For examples, please see US Marine Corps, "Communication Emitter Sensing and Attacking System (CESAS) II," https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/CESAS-II/; and US Naval Air Systems Command, "ALQ-231 Intrepid Tiger Pod," https://www.navair.navy.mil/product/ALQ-231-Intrepid-Tiger-Pod.

115 Sandra Erwin, "US Space Force Declares 'Offensive' Communications Jammer Ready for Deployment," *Space News*, March 15, 2020, https://spacenews.com/u-s-space-force-declares-offensive-communications-jammer-ready-for-deployment/.

116 Jiayu Zhang, "China's Military Employment of Artificial Intelligence and Its Security Implications," *International Affairs Review*, August 16, 2020, https://iar-gwu.org/print-archive/blog-post-title-four-xg-tap.

117 Michael Dahm, "Chinese Debates on the Military Utility of Artificial Intelligence," War on the Rocks, June 5, 2020, https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/.

118 Alina Polyakava, "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare," Brookings Institution, November 5, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

119 Roger McDermott, "Russia's Armed Forces Test and Refine Electronic Warfare Capability," Jamestown Foundation, April 29, 2020, https://jamestown.org/program/russias-armed-forces-test-and-refine-electronic-warfare-capability/.

120 Sam Bendett and Martijn Rasser, "Transcript from Russian Advances in Military Automation and AI," Center for a New American Security, June 4, 2020, https://www.cnas.org/publications/transcript/transcript-from-russian-advances-in-military-automation-and-ai.

121 Daniel Hoadley and Kelley Sayler, "Artificial Intelligence and National Security," Congressional Research Service, November 10, 2020, https://fas.org/sgp/crs/natsec/R45178.pdf.

122 Kyle Mizokami, "The Navy's New AI Missile Sinks Ships the Smart Way," *Popular Mechanics,* February 25, 2016, https://www.popularmechanics.com/military/weapons/a19624/the-navys-new-missile-sinks-ships-the-smart-way/.

123 Mallory Shelbourne, "Navy Testing Battle Management Aid on Aircraft Carrier," USNI News, November 26, 2020, https://news.usni.org/2020/11/26/navy-testing-battle-management-aid-on-aircraft-carrier; Jen Judson and Nathan Stroudt, "At Project Convergence, the US Army Experienced Success and Failure—and It's Happy about Both," *Defense News*, October 12, 2020, https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergence-the-us-army-experienced-success-and-failure-and-its-happy-about-both/; Theresa Hitchens, "ABMS Demo Proves AI Chops for C2," *Breaking Defense*, September 3, 2020, https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

124 Mark Pomerleau, "US Army to Upgrade Bigger Units with New Electronic Warfare Gear," C4ISRNET, October 1, 2020, https://www.c4isrnet.com/electronic-warfare/2020/10/01/us-army-to-upgrade-bigger-units-with-new-electronic-warfare-gear/.

125 Mark Pomerleau, "A New Company-Level Unit to Support Information Warfare," C4ISRNET, July 8, 2020, https://www.c4isrnet.com/information-warfare/2020/07/08/heres-what-tactical-army-cyber-units-will-use-to-conduct-operations/.

126 Engstrom, *Systems Confrontation and System Destruction Warfare*.

127 Hoehn, "U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress."

128 Mark Barrett and Mace Carpenter, *Survivability in the Digital Age: The Imperative for Stealth* (Arlington, VA: Mitchell Institute for Aerospace Studies, 2017), http://docs.wixstatic.com/ugd/a2dd91_cd5494417b644d1fa7d7aacb9295324d.pdf.

129 Jon Lake, "Anti-Ship Missile Evolution," Asian Military Review, January 10, 2020, https://asianmilitaryreview.com/2020/01/anti-ship-missile-evolution/.

130 Cameron Tracy and David Wright, "Modeling the Performance of Hypersonic Boost-Glide Missiles," *Science & Global Security*, 28:3, 135-170, DOI: 10.1080/08929882.2020.1864945.

131 Nathan Strout, "Senate Bill Would Add $120M for Hypersonic Tracking Satellites," C4ISRNET, June 24, 2020, https://www.c4isrnet.com/battlefield-tech/space/2020/06/24/senate-bill-adds-120m-for-hypersonic-tracking-satellites/.

132 Sandra Erwin, "DoD to Test Laser Communications Terminals in Low Earth orbit," *Space News*, June 8, 2020, https://spacenews.com/dod-to-test-laser-communications-terminals-in-low-earth-orbit/.

133 Megan Eckstein, "Flight Tests Begin on Next Generation Jammer Mid-Band Pods; Could Reach Milestone C This Fall," USNI News, August 19, 2020, https://news.usni.org/2020/08/19/flight-tests-begin-on-next-generation-jammer-mid-band-pods-could-reach-milestone-c-this-fall.

134 M. Thomas Davis, David Barno, and Nora Bensahel, "The Enduring Need for Electronic Attack in Air Operations," Center for a New American Security, January 10, 2014, http://www.jstor.com/stable/resrep06162.

135 Valerie Insinna, "This Is How the Air Force Plans on Improving Its Electronic Warfare Capabilities," *Defense News*, September 19, 2019, https://www.defensenews.com/digital-show-dailies/air-force-association/2019/09/19/this-is-how-the-air-force-plans-on-improving-its-electronic-warfare-capabilities/.

136 Shelbourne, "Navy Testing Battle Management Aid on Aircraft Carrier"; DARPA, "Creating Cross-Domain Kill Webs in Real Time," September 18, 2020, https://www.darpa.mil/news-events/2020-09-18a.

137 L3Harris, "Symphony® Communications Manager," https://www.l3harris.com/all-capabilities/symphony.

138 US Department of Defense, Defense Standardization Program Office, "Modular Open Systems Approach (MOSA)," https://www.dsp.dla.mil/Programs/MOSA/; Open Group FACE Consortium, "Future Airborne Capability Environment (FACE)," https://www.opengroup.org/face; Office of the Under Secretary of Defense for Research and Engineering, Director of Defense Research and Engineering for Advanced Capabilities, "Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs," May 2020, https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf.

139 DARPA, "Creating Cross-Domain Kill Webs in Real Time."

Hudson Institute
1201 Pennsylvania Avenue, Fourth Floor, Washington, D.C. 20004
+1.202.974.2400 www.hudson.org