CSBA

Center for Strategic and Budgetary Assessments

WINNING THE INVISIBLE WAR

GAINING AN ENDURING U.S. ADVANTAGE IN THE ELECTROMAGNETIC SPECTRUM

BRYAN CLARK

WHITNEY MORGAN MCNAMARA

TIMOTHY A. WALTON

WINNING THE INVISIBLE WAR

GAINING AN ENDURING U.S. ADVANTAGE IN THE ELECTROMAGNETIC SPECTRUM

BRYAN CLARK

WHITNEY MORGAN MCNAMARA

TIMOTHY A. WALTON

CSBA

Center for Strategic and Budgetary Assessments

2019

ABOUT THE CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS (CSBA)

The Center for Strategic and Budgetary Assessments is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's analysis focuses on key questions related to existing and emerging threats to U.S. national security, and its goal is to enable policymakers to make informed decisions on matters of strategy, security policy, and resource allocation.

ABOUT THE AUTHORS

Bryan Clark is a Senior Fellow at the Center for Strategic and Budgetary Assessments. At CSBA he has led studies in naval warfare, electromagnetic warfare, precision strike, and air defense. In response to the 2016 National Defense Authorization Act, he led one of three Navy fleet architecture studies that assessed the Navy's future needs and the implications of new technologies for fleet design. Prior to joining CSBA, he was Special Assistant to the Chief of Naval Operations (CNO) 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 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. He is the recipient of the Department of the Navy Superior Service Medal and the Legion of Merit.

Whitney Morgan McNamara is a Senior Analyst at the Center for Strategic and Budgetary Assessments. Ms. McNamara was a National Security Fellow at the Woodrow Wilson Center and worked in the Political-Military Bureau at the Department of State and in the Office of the Secretary of Defense for Middle East Policy. She received her M.A. in Strategic Studies and International Economics from the Johns Hopkins School of Advanced International Studies where she was a Bradley Fellow and a Presidential Management Fellowship Finalist. Prior to that, Whitney spent four years working in the Middle East as a project manager and consultant. She has written for or been quoted in The Washington Post, Cipher Brief, RealClear Defense, Breaking Defense, C4ISRNET, Aspen Review, Al-Monitor, Al Arabiya, Jordan Business and Middle East Online.

Timothy A. Walton is a Research Fellow at the Center for Strategic and Budgetary Assessments. Mr. Walton focuses his research and analysis on the development of new operational concepts, trends in future warfare, and Asia-Pacific security dynamics. Mr. Walton has authored a number of publications on Chinese military doctrine and capabilities, regional security dynamics, and U.S. force planning. Prior to joining CSBA, he was a Principal of Alios Consulting Group and an Associate of Delex Systems. He has a Bachelor's in International Politics with a concentration in Security Studies from the Walsh School of Foreign Service at Georgetown University, and Master's degree in Security Studies from the same institution.

ACKNOWLEDGMENTS

The authors would like to thank Melinda and Steve Tourangeau, who wrote appendices to this report that were part of the original report to Congress upon which this report is based. The authors would also like to express their appreciation to those in the defense and broader electromagnetic spectrum community whose insights enriched this report. In particular they would like to thank John "Hap" Arnold, Karl Dahlhauser, and Anna Jimenez for supporting research during this project. The authors would also like to thank the CSBA staff for their assistance with this report. Special thanks go to Thomas G. Mahnken and Evan Montgomery for their thoughtful review of the draft report and to Kamilla Gunzinger for her editing and publication support.

CSBA receives funding from a broad and diverse group of contributors, including private foundations, government agencies, and corporations. A complete list of these organizations can be found on our website at www.csbaonline.org/about/contributors.

This material is based upon work supported by the Defense Technical Information Center under Contract No. FA8075-14-D-00018.

Cover: An Air Force Research Laboratory (AFRL) photo of a laser that can help reduce atmospheric distortion. The Air Force uses it to better photograph passing spy satellites.

Contents

FIGURES

CHAPTER 1

Introduction

The electromagnetic spectrum (EMS) is increasingly central to modern life. For more than a century, broadcast or satellite radio and television have provided entertainment, news, and propaganda to mass audiences. During the last three decades, mobile computing and communications became many people's main way to connect with others and share information. Now, the advent of small, inexpensive antennas and processors is enabling a virtual explosion of new sensors, communications, and related applications operating in the EMS. Cars, trucks, trains, ships, and aircraft are incorporating a growing array of radar, infrared (IR), or visual sensors to automate more functions and help operators navigate complex situations. Almost every new electronic device, from toasters to computers, is equipped with a radio to communicate its status and receive direction. And today's patchwork of 4GLTE and local wi-fi networks will soon give way to high-bandwidth, low-latency 5G mobile communications.

Militaries are taking advantage of emerging sensor and communication technologies. During the 20th century, armed forces improved their performance and security by either developing their own dedicated EMS systems or buying and integrating those of allies. Today, commercial EMS technologies are widely available and outperform military capabilities in some applications. As a result, militaries are incorporating commercial EMS technologies into military sensors, communication systems, and jammers or simply using commercial systems to "hide in plain sight."

The proliferation and growing sophistication of civilian and military EMS capabilities has resulted in an increasingly congested and contested electromagnetic environment for which the U.S. military is unprepared. Over the past decade, several government and external assessments found that the U.S. military is falling behind Chinese and Russian forces in electronic warfare (EW) and that U.S. forces will be challenged to achieve EMS superiority in future conflicts.[1] To address these concerns, the U.S. Department of Defense (DoD)—sometimes under Congressional direction—initiated an ongoing series of actions to improve its EW doctrine and capabilities. This study will argue these efforts have been unfocused and are likely to fail at delivering EMS superiority, and that a more strategic approach is needed to guide DoD EW and Electromagnetic Spectrum Operations (EMSO) initiatives.

Throwing Money at the Wrong Solutions

DoD began a sustained effort earlier this decade to improve its EW and EMSO concepts and capabilities. The DoD Chief Information Officer (CIO) issued an Electromagnetic Spectrum (EMS) Strategy in 2013, which described improved approaches for the U.S. military to manage and coordinate operations in the EMS.[2] The Joint Staff complemented the new strategy by leading the development of new operational concepts for EMSO and electromagnetic battle management (EMBM).[3]

In response to a Defense Science Board study and subsequent Congressional direction, DoD established an EW Executive Committee (EXCOMM) in 2015 to oversee EW doctrine and capability development, personnel management, and readiness.[4] In 2017, the EW EXCOMM published an EW Strategy, which described the actions and orchestration needed to:

- Organize the EW enterprise to ensure EMS superiority;
- Train and educate U.S. forces for 21st Century EW and EMS operations;
- Equip the force with agile, adaptive, and integrated EW capabilities; and
- Bolster partnerships with industry, academia, interagency and allied partners.[5]

1 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), available at 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: U.S. Library of Congress, 2012), available at https://www.gao.gov/assets/600/592211.pdf; Madison Creery, "The Russian Edge in Electronic Warfare," *Georgetown Security Review*, June 26, 2019, available at 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, available at https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf?mtime=20190531090041.

2 DoD CIO, *Electromagnetic Spectrum Strategy: A Call for Action* (Washington, DC: DoD, 2013), available at https://archive.defense.gov/news/dodspectrumstrategy.pdf.

3 U.S. Joint Staff, *Joint Publication 6-1: Joint Electromagnetic Spectrum Management Operations* (Washington, DC: 2012, DoD), available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_01.pdf.

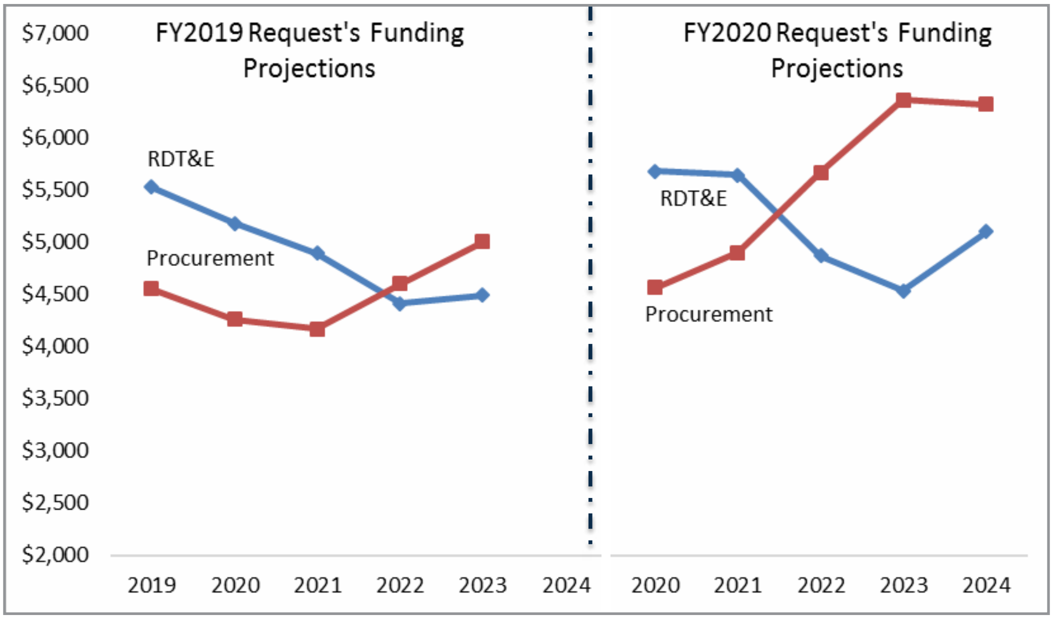
4 DSB, *21st Century Military Operations in a Complex Electromagnetic Environment*; and DoD, "Electronic Warfare Policy," DoD Directive 3222.04, Washington Headquarters Services, March 26, 2014, available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/3222.04.pdf?ver=2018-10-11-075832-267.

5 AT&L/Tactical Warfare Systems/EW Programs Office, *The DoD Electronic Warfare Strategy* (Washington, DC: DoD, 2017), pp. 7–11.

Notably, the EW strategy did not address new operational approaches for EW and EMSO and instead focused on strengthening the technical, organizational, and human capital foundations for DoD's EW and EMSO enterprise.[6]

DoD increased funding for EW and EMSO starting in FY 2017 in concert with the new strategy. Budget increases continued through the President's proposed FY 2020 budget, in which research, development, test, and evaluation (RDT&E) funding for EW capabilities grew by 9.7 percent and EW procurement funding increased by 7.1 percent compared to the FY 2019 program. Overall, DoD EW funding in the proposed FY 2020 budget was $10.1 billion, an amount on par with the F-35 Lightning II strike-fighter or *Gerald Ford*-class aircraft carrier programs.[7]

FIGURE 1: EW RDT&E AND PROCUREMENT FUNDING



Hoehn, *U.S. Military Electronic Warfare Investment Funding*.

The growth in DoD EW spending, however, is not guided by a coherent vision of how U.S. forces would operate and fight in the EMS and is unlikely to yield significant improvements against China and Russia, the U.S. military's most challenging competitors. New networked, cognitive, and agile EW technologies called for in the 2017 EW Strategy have been slow to transition into operational systems, and RDT&E spending to field those capabilities is

6 John McHale, "Funding for Radar, Electronic Warfare, C4ISR, Steady in DoD FY 2017 budget request," Military Embedded Systems, available at http://mil-embedded.com/4894-funding-for-radar-electronic-warfare-c4isr-steady-in-dod-fy-2017-budget-request/.

7 John R. Hoehn, *U.S. Military Electronic Warfare Investment Funding: Background and Issues for Congress* (Washington, DC: Congressional Research Service [CRS], June 6, 2019).

projected to decrease for several years after FY 2020. Although EW procurement is projected to rise through 2024, it is concentrated in a few platform-centric programs such as the ALQ-249 Next Generation Jammer and SLQ-32 Shipboard EW Improvement Program. These systems update existing programs but do not fundamentally change the way U.S. forces operate in the EMS and represent a traditional move-countermove approach to military capability development.

The lack of an operational EW or EMSO strategy, combined with shrinking RDT&E funding and increased spending on legacy system upgrades, will likely result in EW and EMSO improvements that are too incremental to allow the United States to regain the upper hand in competitions with the Chinese and Russian militaries.

The Need for a Strategic Assessment

To address the slow improvement in DoD EW and EMSO capabilities, Congress established an EMSO Cross-Functional Team (CFT) in the 2019 National Defense Authorization Act (NDAA) as a temporary governance body with authorities to propose changes to DoD EMSO doctrine, plans, and programs.[8] The 2019 NDAA also directed DoD to arrange for an independent assessment of its EW plans and programs by a group outside DoD that would include the following elements:

- Assess the strategies, programs, order of battle, and doctrine of the Department of Defense related to the electronic warfare mission area and electromagnetic spectrum operations;
- Assess the strategies, programs, order of battle, and doctrine of potential adversaries, such as China, Iran, and the Russian Federation, related to the same;
- Develop recommendations for improvements to the strategies, programs, and doctrine of the Department of Defense in order to enable the United States to achieve and maintain superiority in the electromagnetic spectrum in future conflicts; and
- Develop recommendations for the Secretary, Congress, and such other federal entities as [the contractor] considers appropriate, including recommendations for:
    - Closing technical, policy, or resource gaps;
    - Improving cooperation and appropriate integration within the Department of Defense entities;
    - Improving cooperation between the United States and other countries and international organizations as appropriate; and

8 Patrick Shanahan, Acting Secretary of Defense "Establishment of the EMS Operations Functional Team," memorandum, February 2, 2019, p. 2.

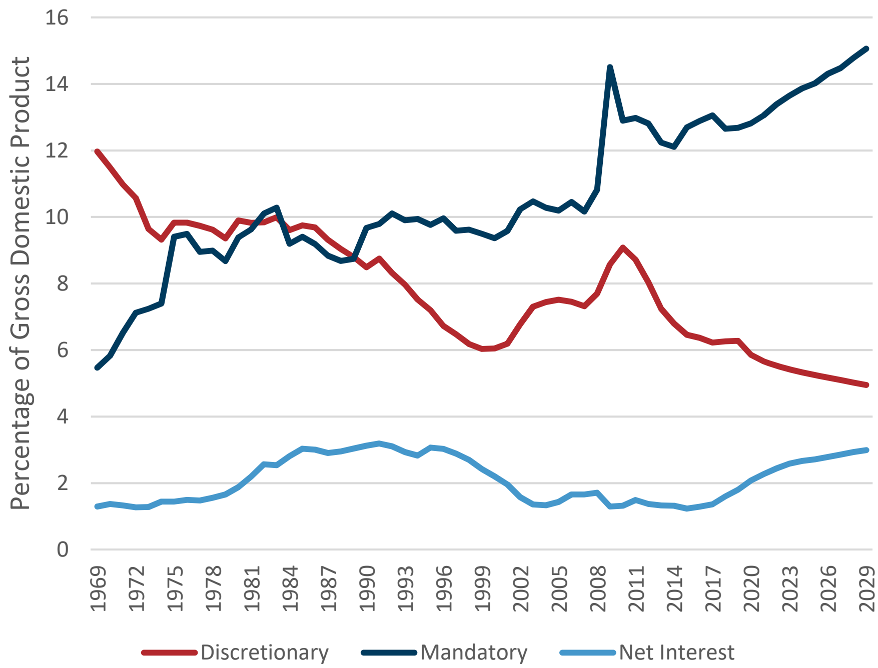
- Such other important matters identified that are directly relevant to the strategies of the Department of Defense.

A common methodology for this assessment would be to catalogue and propose solutions for gaps between U.S. and competitor EW or EMSO concepts and capabilities. For example, a gap-focused approach is directed for Capability Based Assessments (CBA) conducted under DoD's Joint Capabilities Integration and Development System (JCIDS).[9] This technique, however, requires assumptions regarding adversary operational concepts and tactics that may prove incorrect and projects future U.S. concepts forward into a future in which they may not apply.

The most problematic aspect of a gap-based assessment is it tends to result in a "laundry list" of recommended solutions to symmetrically solve each identified gap instead of identifying ways the U.S. military could gain a more enduring advantage against adversaries by changing its own strategy and operational concepts. This approach cedes the capability development initiative to the adversary, and DoD may require a decade or more to fill the identified gaps, during which time adversaries may adopt new concepts and capabilities. Given the shortfalls identified by previous studies of DoD EW and EMSO capabilities, a gap-based assessment would also likely recommend increased investment in EW and EMSO capabilities relative to today. As noted above, EW spending increased until FY 2020 and is expected to be flat or lower during the next several years. It is unlikely this trajectory will change in the near-to-mid-term as defense budgets come under pressure by higher mandatory spending on federal debt service and social programs, combined with the growing cost to operate and maintain U.S. forces.

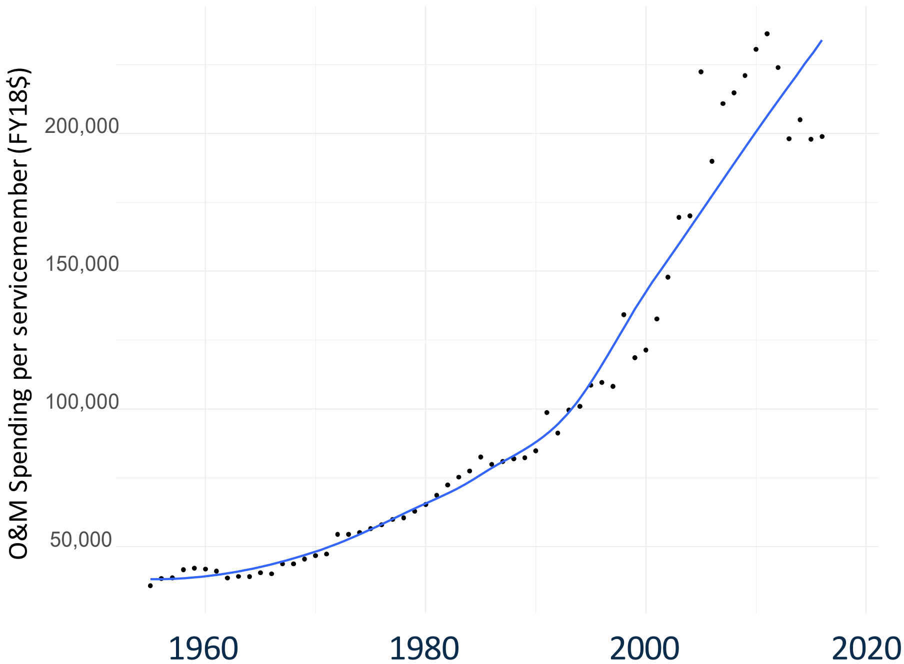
9 Joint Staff, *Charter of The Joint Requirements Oversight Council (JROC) and Implementation of The Joint Capabilities Integration and Development System (JCIDS)*, CJCSI 5123.01H (Washington, DC: U.S. Joint Staff, August 31, 2018), pp. D-1–D-3, available at http://acqnotes.com/wp-content/uploads/2018/11/CJCSI-5123.01H-Charter-of-the-Joint-Requirements-Oversight-Council-JROC-and-Implementation-of-the-JCIDS-31-Aug-2018.pdf.

FIGURE 2: COSTS TO SERVICE THE FEDERAL DEBT AND SUPPORT MANDATORY SPENDING ON SOCIAL PROGRAMS IS PREDICTED BY THE CONGRESSIONAL BUDGET OFFICE (CBO) TO CROWD OUT DISCRETIONARY SPENDING, INCLUDING THAT ON DEFENSE, DURING THE NEXT DECADE



Congressional Budget Office (CBO), The Budget and Economic Outlook: 2019 to 2029, (Washington, DC: CBO, 2019), p. 5, available at https://www.cbo.gov/publication/54918.

FIGURE 3: U.S. MILITARY OPERATIONS AND MAINTENANCE (O&M) COSTS ARE INCREASING FOR EACH PLATFORM OR PIECE OF EQUIPMENT, AS MEASURED BY O&M COSTS PER SERVICE MEMBER



Office of the Undersecretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2019* (Green Book), available at https://comptroller.defense.gov/Budget-Materials/Budget2019/; and Defense Manpower Data Center (DMDC), "DoD Personnel, Workforce Reports & Publications," available at https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp.

Rather than comparing U.S. EW and EMSO capabilities with those of potential adversaries and identifying a set of gaps or shortfalls, this study takes a more holistic approach by identifying the key asymmetries between U.S. and competitor EW and EMSO strategies, concepts, capabilities, and programs. The study uses asymmetries to identify opportunities for U.S. forces to gain an advantage in the EMS, challenges DoD should attempt to overcome, and shortfalls DoD is unlikely to eliminate and should only attempt to mitigate. This overall approach is often described as "net assessment" by its practitioners.[10]

Implementing the recommendations from a net assessment will incur risks, as some individual threats or gaps may be left unaddressed in favor of developing capabilities that undermine important adversary strengths or exacerbate its perceived vulnerabilities.

10 See, for example, James G. Roche and Thomas G. Mahnken, "What is Net Assessment?" in Thomas G. Mahnken, ed., *Net Assessment and Military Strategy: Retrospective and Prospective Essays* (Amherst, NY: Cambria Press, forthcoming in 2020); Eliot Cohen, "Net Assessment: An American Approach," JCSS Memorandum no. 29, April, 1990, available at https://www.inss.org.il/publication/net-assessment-an-american-approach/; George E. Pickett, James G. Roche, and Barry D. Watts, "Net Assessment: A Historical Review," and Stephen Peter Rosen, "Net Assessment as an Analytical Concept," in A.W. Marshall, J.J. Martin, and Henry S. Rowan, eds., *On Not Confusing Ourselves* (Boulder, CO: Westview Press, 1991); and Paul Bracken, "Net Assessment: A Practical Guide," *Parameters*, Spring 2006.

However, a net assessment approach is well suited to today's long-term competition between the United States, China, and Russia. Both U.S. competitors are pursuing territory and influence along their periphery using a combination of sustained political and hybrid warfare to coerce or destabilize their neighbors. In contrast, the Soviet Union's campaign to be the predominant power during the Cold War was global in scope and relied to a much greater degree on combat operations. In general, the Soviet approach was more dependent on imposing attrition than today's Chinese and Russian operations, which are designed to achieve success through superior decision-making. As a result, a net assessment's identification of opportunities to attack an adversary's perceived strengths and vulnerabilities may be a better analytic approach for today's competition compared to traditional campaign analysis or modeling and simulation that identifies gaps in the ability of forces to impose attrition.[11] Policy recommendations emerging from a net assessment approach may offer a faster and more affordable way to regain an EMS advantage than methodically and incrementally countering new threats with modestly improved U.S. EW and EMSO systems.

Chapter 2 of this study offers a net assessment of U.S., Chinese, and Russian EW and EMSO doctrine, trends, and asymmetries and highlights some of their implications. Chapter 3 provides recommendations for DoD to apply the net assessment's findings toward gaining an advantage in the EW and EMSO competition with China and Russia.

11 James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: DoD, 2018), p. 7; and Eric Edelman and Gary Roughead, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: U.S. Institute of Peace, 2018); and Hal Brands, "The Lost Art of Long-Term Competition," *The Washington Quarterly* 41, no. 4, January 2019.

CHAPTER 2

Net Assessment of U.S., Chinese, and Russian doctrine and programs in the EMS

A comprehensive analysis of the EW and EMS concepts, programs, and capabilities fielded or being pursued by the United States and its adversaries, the resulting gaps, and proposed solutions is beyond the scope of this study. Moreover, such an assessment, if undertaken, would not necessarily be helpful to U.S. policymakers. Building U.S. EW and EMSO plans to fill anticipated capability gaps assumes current tactics and operational concepts will be employed in the future and cedes the initiative for EMS capability development to China and Russia. Fully mitigating all EW or EMSO capability gaps may also be infeasible within the fiscal and temporal constraints facing DoD and the U.S. government.

In contrast, this study argues that DoD should pursue a more proactive and strategic approach than simply building or revising U.S. EMS capabilities to avoid every adversary jammer or passive sensor while targeting each opposing EM system. For example, the top priority of current U.S. defense strategy is deterring great powers through the credible ability to delay, degrade, or deny an act of aggression against U.S. allies or partners. Rather than solving every capability gap, DoD should focus its EW and EMSO concept and capability development on the highest leverage opportunities to reduce the confidence of great power militaries that an act of aggression will be successful.

DoD's plans for EMS operations should also reflect the long-term nature of great power competition. Although discrete U.S. EMS capabilities or tactics could undermine a competitor's confidence in its plans, it is also possible, even likely, that a competitor could eventually mitigate the impact of these investments with relatively modest changes in its tactics or systems. U.S. planning for EMS operations should instead seek to identify and exploit enduring sources of U.S. advantage that would be costly or time-consuming for an opponent to change or overcome, such as alliances, geography, culture, or force design.

The focus of this study on great powers China and Russia is also deliberate. The EW and EMSO concepts and capabilities of potential regional adversaries such as Iran and North Korea are derived from technologies and tactics provided by the Chinese or Russian militaries.[12] Although these regional powers have nearly the same level of capability as Chinese and Russian militaries in some missions, such as GPS or communications jamming,[13] they have not exceeded great power EW or EMSO capabilities and also possess a much less comprehensive EW or EMSO portfolio.[14] Therefore, from the perspective of a capability gap assessment, Iran and North Korea can be considered less-included cases of China and Russia. In the context of a net assessment, the geostrategic locations of these regional competitors create different asymmetries compared to China or Russia, but are similar enough as to not require a separate analysis.

The Net Assessment Framework

To support a holistic approach to DoD EMS force development and operations, this study will use the net assessment framework pioneered by Andrew Marshall at the National Security Council and later developed by the DoD Office of Net Assessment he led for more than four decades.[15] Although there is no fixed methodology for conducting a net assessment, in general it would study how each subject nation or military planned to compete institutionally and operationally, its means of doing so, and the perception of each nation's leaders regarding their position relative to their competitors.[16]

The net assessment framework used in this study will consider three sets of characteristics of the U.S., Chinese, and Russian militaries regarding their use of EW and EMS operations.

- Doctrine: Each countries' national strategies and the role and employment of EW and EMS operations within those strategies;
- Trends: Capability trends and organization and institutional support to EMS capabilities; and

12 Drago Bosnić, "Russia Delivers Electronic Warfare Systems to Iran," *Checkpoint Asia*, August 9, 2019.

13 Siobhán O'Grady, "This Isn't the First Time U.S.-Iran Feuds Have Involved a Drone," *Washington Post*, June 22, 2019.

14 Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure," *Military Review,* July-August 2019.

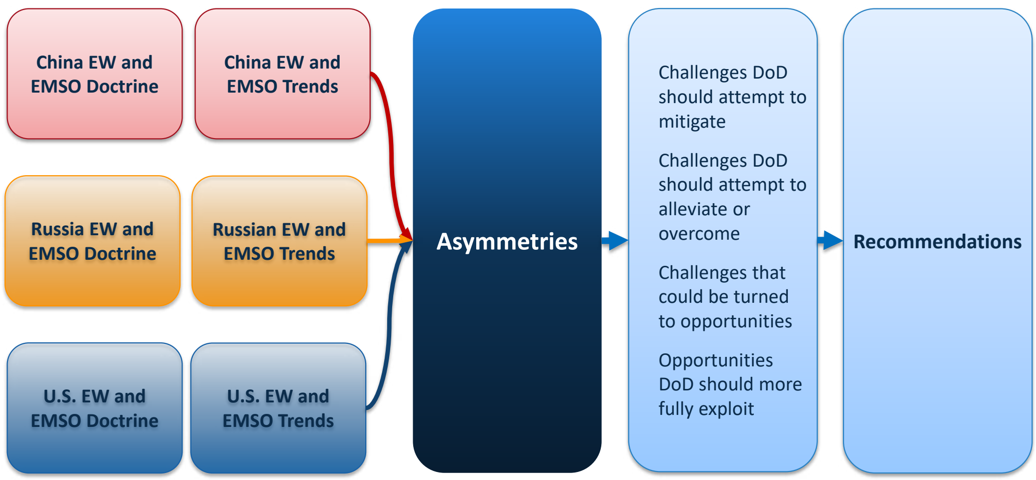
15 Andrew F. Krepinevich, "Measures of Power: On the Lasting Value of Net Assessment," *Foreign Affairs*, April 19, 2019.

16 Jacob Cohn, Adam Lemon, and Evan Braden Montgomery, *Assessing the Arsenals: Past, Present, And Future Capabilities* (Washington, DC: Center for Strategic and Budgetary Assessments, 2019), pp. 2–3.

- Asymmetries: Areas where one competitor's approach, capabilities or characteristics create significant threats or opportunities for the other competitors. These could include differences in doctrine and capabilities or fundamental factors such as geography, demographics, or alliances.[17]

These characteristics will be used to reveal challenges and opportunities for DoD to address and formulate a set of recommendations that are designed to exacerbate adversaries' perceived vulnerabilities and undermine confidence in their perceived strengths.[18]

FIGURE 4: A NET ASSESSMENT IDENTIFIES ASYMMETRIES BETWEEN COMPETITORS' DOCTRINE AND CAPABILITY TRENDS AND PROPOSES SOLUTIONS TO EXPLOIT OPPORTUNITIES AND MITIGATE SHORTFALLS



The discussion that follows summarizes aspects of U.S., Russian, and Chinese EW and EMSO doctrine, capabilities, programs, and forces that are most relevant to the long-term competition between them. For this analysis, EW is assumed to comprise electronic attack (EA), including directed energy, electronic support (ES), and electronic protection (EP). EMSO is assumed to include EW and C3ISR (command and control, communications, intelligence, surveillance, and reconnaissance) activities that occur in the EMS.

17 This framework is adapted from Thomas Skypek, "Evaluating Military Balances Through the Lens of Net Assessment: History and Application," *Journal of Military and Strategic Studies* 12, no. 2, Winter 2010; Paul Bracken, "Net Assessment: A Practical Guide," *Parameters*, Spring 2006; and Cohen, "Net Assessment."

18 Net assessments often use scenarios to evaluate doctrine, trends, and asymmetries dynamically, as well as to assess the perceptions held by each country's decision-makers. Scenarios are evaluated using wargames, tabletop exercises, or other interactive methods. Due to the limited time allotted to conducting this study, scenario analysis will be conducted as a follow-on effort.

Doctrine

The ways in which the PLA and Russian Armed Forces plan to use actions in the EMS to support their operations may yield challenges and potential opportunities for U.S. EW and EMSO concepts and capabilities. The U.S. National Defense Strategy (NDS) and Congressionally mandated NDS Commission both argue that the United States is in a long-term competition with China and Russia.[19] Therefore, this study will focus on the operational doctrine and EMS concepts of the United States, China, Russia rather than current tactics. And because strategy and doctrine can evolve over time, this study will also consider a broader set of factors, including a competitor's technological and industrial base, geography, demographics, and force structure, which constrain the degree to which a competitor's EW and EMSO concepts can change.[20]

China

During the six decades since the founding of the People's Republic of China (PRC), the People's Liberation Army (PLA) has consistently increased the emphasis its military doctrine places on information. Chinese military thinking has transitioned from viewing information as an enabler of warfare to viewing it as the main line of military effort in a way that has mirrored DoD's own evolution toward network-centric warfare. Network-centric warfare concepts were first discussed during the 1990s and implemented during U.S. operations since 2001 in Iraq, Afghanistan, and Syria.[21] For example, whereas China's 2004 defense white paper emphasized "Local Wars Under Informationized Conditions," the 2015 version called on PLA units to be ready to fight "Informationized Local Wars."

The PLA's 2019 defense white paper goes one step further by identifying the next phase of warfare as "Intelligentized," in which military organizations harness information through artificial intelligence (AI) to permit more rapid and effective planning and execution of military operations.[22] Although some military thinkers in the United States view AI as a tool to enable junior commanders to operate independently, it is likely the PLA's leaders consider AI to be a

19 Mattis, *Summary of the 2018 National Defense Strategy*, p. 7; and Edelman and Roughead, *Providing for the Common Defense*.

20 Brands, "The Lost Art of Long-Term Competition."

21 Shitanshu Mishra, "Network Centric Warfare in the Context of 'Operation Iraqi Freedom'," *Strategic Analysis* 27, no. 4, 2003.

22 Elsa Kania, "Innovation in the New Era of Chinese Military Power," *The Diplomat,* July 25, 2019.

way to improve the ability of senior commanders to build plans that humans or machines will autonomously execute throughout a force.[23]

The desire of Chinese defense leaders to field a system of systems (SoS) that is capable of defeating an enemy without relying on the creativity of individual operators is a reflection of the PLA's concept of System Destruction Warfare. According to this approach, the PLA's equipment, platforms, organizations, and operators are formed into systems designed to conduct different military functions such as gathering information or delivering fires. The design of each system, and the combination of systems, is intended to create desired effects and address likely threats using centralized, consensual decision-making. Commanders would use information and intelligence systems to consider the situation, identify possible courses of action, and implement plans, including possible branches and sequels, before an operation begins. The SoS and its human operators would then execute the plans.[24]

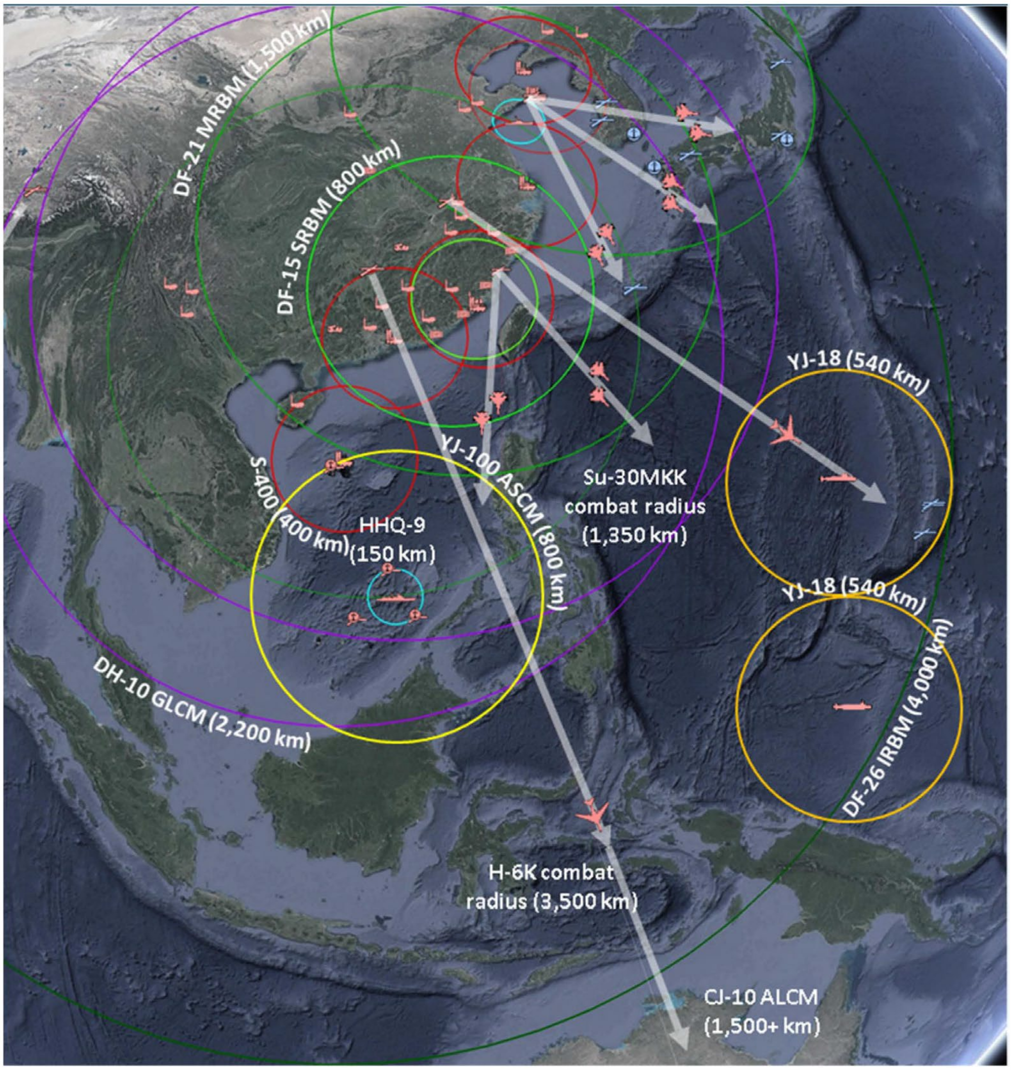
The elements and architecture of PLA forces in System Destruction Warfare are focused on defeating the U.S. military, which the PLA perceives to be the pacing threat and a model to guide PLA force planning. PLA systems within the concept are designed to target specific vulnerabilities the PLA perceives in U.S. systems and operational concepts. For example, a strategic and operational-level vulnerability of U.S. forces is the fact that the United States would have to project power over great distances in any confrontation with the PLA in the Western Pacific. Although the U.S. military has bases in Japan, South Korea, and Guam, they are dependent on exterior lines of communication and all within range of long-range PLA precision weapons. At the operational and tactical level, System Destruction Warfare identifies U.S. communication links as high priorities for PLA jamming or deception.[25]

23 Elsa Kania, "China's Quest for an AI Revolution in Warfare," *Strategy Bridge*, June 8, 2017; John Dotson and Alexander Wang, "The 'Algorithm Game' and Its Implications for Chinese War Control," *Jamestown Foundation China Brief,* April 9, 2019, available at https://jamestown.org/program/the-algorithm-game-and-its-implications-for-chinese-war-control/; and Cortez A. Cooper, "PLA Military Modernization: Drivers, Force Restructuring, and Implications," testimony to the U.S.-China Economic and Security Review Commission, February 15, 2018, available at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT488/RAND_CT488.pdf.

24 Jeff Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND Corporation, 2018), p.27.

25 Work and Grant, *Beating the Americans at their Own Game*, p. 7.

FIGURE 5: CHINA'S LONG-RANGE SENSOR AND WEAPON NETWORK



Data to build this graphic derived from IHS Jane's (2019); and OSD, Military and Security Developments Involving the People's Republic of China 2018.

The relatively static and inflexible nature of PLA military systems and SoS and the PLA's continued reliance on centralized, consensual decision-making may create opportunities that U.S. forces could exploit through EMS operations. Furthermore, the use of AI by the PLA may magnify, rather than mitigate, this potential opportunity by reinforcing centralization and structure in PLA decision-making.

Russia

The development of Russian military's operational concepts is more dynamic than that of China, with the newest approaches emerging from the constant experimentation and real-world experience of Russian forces, as well as large-scale exercises.[26] New approaches to electronic and cyber warfare and local precision reconnaissance and strike developed in Syria and Ukraine are complemented in Russian Armed Force doctrine by evolving concepts for "deep battle," or long-range strike; "active restraint," or deterrence; and "information confrontation," or information warfare.[27]

The Russian concept of information confrontation is the one most relevant to competition between the U.S. and Russian militaries in the EMS. Although often assumed to relate mostly to computer network operations, information confrontation concerns all aspects of information gathering, transmission, and use by an adversary government and military force. Authoritative writings from Russian military leaders identify electronic warfare as a key element of gaining information superiority over an opposing military, both operationally and strategically through information campaigns.[28]

The Russian military seeks to create a comprehensive electronic warfare SoS, not unlike the PLA, designed to comprehensively defeat the U.S. military's C4ISR networks.[29] To that end, Russian ground forces are receiving new EW equipment down to the company level that has performed effectively against U.S. and allied forces in Syria. The Russian military's efforts to improve EW and EMS operations among its naval and air forces have made less progress and may hinder its ability to achieve the level of comprehensive EMS superiority Russian military leaders desire.[30]

Russia's evolving military concepts serve a relatively stable strategy, which emphasizes readiness, non-nuclear deterrence, and the ability to inflict unacceptable damage on an enemy.[31] The strategy's priorities are reflected in the Russian military's frequent snap exercises that help facilitate and demonstrate the readiness of Russian forces in conventional and nuclear operations, including EW and EMSO. Russian military strategy is also represented by its fielding of several new conventional strike missiles that exceed the limits of the now-abrogated Intermediate Nuclear Forces (INF) treaty. These missiles could both support non-nuclear

26 Phillip A. Karber, "Russia's 'New Generation Warfare'," *NGA.mil,* June 4, 2015, available at https://www.nga.mil/MediaRoom/News/Pages/Russia%27s-%27New-Generation-Warfare%27.aspx.

27 Defense Intelligence Agency (DIA), *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: DIA, 2017), p. 23, available at https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937.

28 Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, Estonia: International Centre for Defence and Security, September 2017), pp. 2–3; and "Electronic Warfare Chief Interviewed," *Russia Defense Policy*, May 30, 2017, available at https://russiandefpolicy.blog/tag/yuriy-lastochkin/.

29 DIA, *Russia Military Power*, p. 42.

30 Madison Creery, "The Russian Edge in Electronic Warfare," *Georgetown Security Review*, June 26, 2019.

31 DIA, *Russia Military Power*, p. 17.

deterrence and create the possibility of inflicting unacceptable damage on nearby NATO countries in Eastern and Central Europe.[32]

The Russian military faces significant challenges in fielding next generation EMS technologies and training the personnel to operate them due to an aging, corrupt, and inefficient industrial base and a force that comprises 50 percent conscripts.[33] Moreover, despite the rapid improvements in EW units seen among ground forces, only a portion of Russia's shrinking military benefits from new systems and operational experience because many units, ships, and aircraft do not rotate to the front line for modernization and operations.[34] This could create opportunities for DoD to gain an advantage by fielding next-generation EMS systems and adopting EW and EMSO operational concepts that undermine Russian approaches to deep battle and reconnaissance-strike.

United States

The 2018 U.S. NDS directs DoD to deter great power aggression by demonstrating the ability to delay, degrade, or deny adversary military actions against the United States or its allies.[35] The emphasis on deterrence through denial rather than punishment emerges in part from the fact that Chinese and Russian military forces are much closer to the likely objects of their aggression—such as Taiwan for China and the Baltic states for Russia—than U.S. forces. Being adjacent to potential targets enables the Russian Armed Forces or PLA to establish, on friendly territory, long-range sensor and weapon networks that can support acts of aggression as well as slow or stop intervention from the United States or other allies.[36]

Supported by precision sensor and weapon networks, Chinese or Russian forces could launch an attack and consolidate their gains before U.S. or allied forces could arrive. Presented with a *fait accompli*, U.S. and international leaders may lack an acceptable opportunity to overturn the new status quo through a counter-invasion. This dynamic was recently demonstrated by the Russian annexation of Crimea from Ukraine in 2014.[37]

Shifting the U.S. military's objectives to delaying, degrading, or denying aggression seeks to raise the potential cost and uncertainty associated with an adversary's military adventurism.

32 Amy F. Woolf, *Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress* (Washington, DC: CRS, updated August 2, 2019).

33 Stratfor Worldview, "Russia's Defense Industry Finds Itself in a Tailspin," *RealClearDefense*, May 2, 2019; and Paul Goble, "2018 Spring Draft Highlights Russia's Demographic Decline," *Eurasian Daily Monitor* 15, no. 54, April 10, 2018.

34 Dmitry Gorenberg, "Russia's Military Modernization Plans: 2018–2027," *PONARS Eurasia,* November 2017.

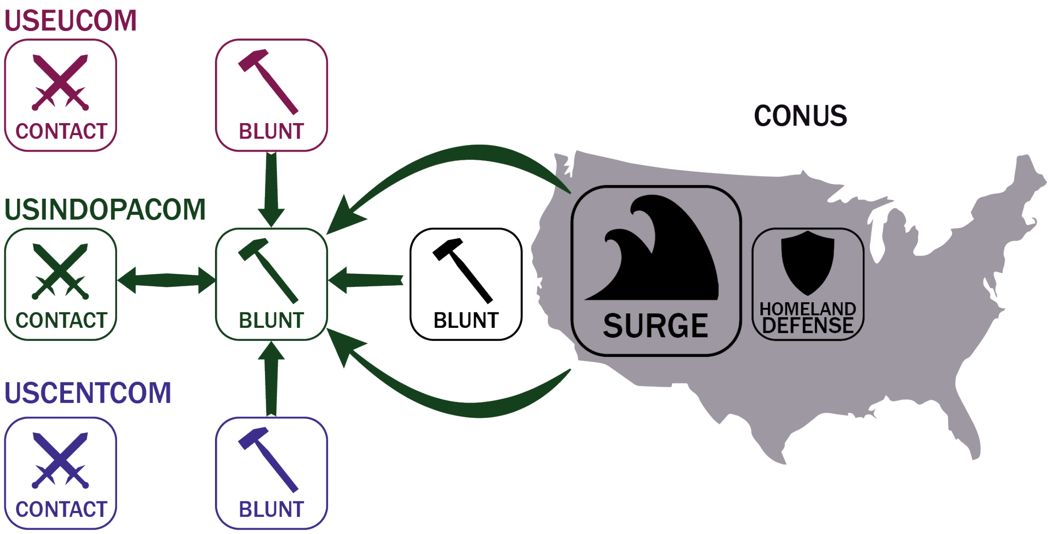
35 Mattis, *Summary of the 2018 National Defense Strategy*, p. 2.

36 DIA, *Russia Military Power*; Office of the Secretary of Defense (OSD), *Military and Security Developments Involving the People's Republic of China 2019*, Annual Report to Congress (Washington, DC: DoD, 2019), available at https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

37 Steven Pifer, "Five Years After Crimea's Illegal Annexation, the Issue Is No Closer to Resolution," *Order From Chaos*, blog, March 18, 2019.

In support of this approach, the 2018 NDS prescribes a new posture model that places U.S. forces in proximity to potential adversaries and targets to allow prompt intervention on behalf of allies and partners.

FIGURE 6: POSTURE MODEL PRESCRIBED BY THE 2018 NDS PLACES FORCES IN A CONTACT, BLUNT, OR SURGE LAYER



In the NDS posture model, deployed forces operate in two layers. The most forward forces are in the "Contact" layer that interacts regularly with allies and adversaries. These would be the first to respond in the event of conflict. Units operating farther from allies and adversaries are in the "Blunt" layer and are the forces that would come to the immediate assistance of Contact layer forces during a military response. Forces in the Contact layer would include ships at sea, aircraft in the air or deployed away from their home station, and troops on the ground outside a base or rear area. Blunt layer units would consist of those at U.S. bases forward or able to deploy rapidly from the continental United States (CONUS).[38]

EMS superiority will be a necessary enabler of U.S. defense strategy and the associated posture model. For U.S. forces to survive in a contested area close to adversaries and potential targets, units will need to be able to reduce the effectiveness of enemy surveillance and tracking, rapidly identify potential targets, and defeat large volumes of precision weapons on short notice. These requirements will place a premium on ES to find enemy forces and incoming weapons, EA to degrade or destroy sensors and weapons, and EP to prevent or minimize enemy exploitation of U.S. or allied communications and defeat of friendly sensors.

Prior to the 2018 NDS, DoD published an EMS Strategy in 2013 and an Electronic Warfare Strategy in 2017. The EMS Strategy developed by the DoD CIO sets an ambitious vision of

38 Mattis, *Summary of the 2018 National Defense Strategy*, p. 7.

gaining spectrum access when and where it is needed but only addresses spectrum management within DoD and between DoD and civilian users. This is an essential element of EMS superiority, but represents “table stakes” in great power competition. The more challenging task is gaining EMS access against a capable opponent, which is the focus of the EW Strategy. Although notionally centered on EA, ES, and EP, the EW Strategy establishes four main goals for DoD EMS operations:

1. Organize the EW enterprise to ensure EMS superiority;
2. Train and educate U.S. forces for 21st Century EW and EMS operations;
3. Equip the force with agile, adaptive, and integrated EW capabilities; and
4. Bolster partnerships with industry, academia, interagency and allied partners.

DoD’s EW doctrine and programs have yet to achieve these goals or fully enable execution of the 2018 NDS through the EMS. DoD has made significant progress on some goals, such as organizing the EW enterprise and bolstering partnerships. Partial progress was made toward training and educating the EW and EMS workforce, with practical training and exercises for EW operators being the most significant shortfall. DoD has made significant strides in developing technology for agile, adaptive, and integrated EW and EMS operations, but these technologies are not being transitioned into acquisition programs quickly enough.[39] The EW strategy is currently being revised by the EMSO Cross-Functional Team (CFT) to better align it with the 2018 NDS.

Trends

China, Russia, and the United States have developed organizations to implement their strategies by assessing future EW and EMS needs, develop new EW and EMS capabilities, operate systems, and train and evaluate units conducting EW and EMS operations. The capabilities fielded by each competitor reflect their particular view of how they should operate in the EMS to pursue their military objectives. Although the Chinese, Russian, and U.S. militaries all improved their ability to operate in and control the EMS during the last decade, the manner in which China and Russia have organized and equipped their forces may provide opportunities for DoD to gain an advantage.

China

To improve its ability to implement a strategy of informationized, and eventually intelligentized, warfare, in 2015 the PLA reorganized most of its forces that gather and disseminate information, as well as those that control adversaries’ access to accurate information, under

39 See Bryan Clark and Whitney McNamara, *Electronic Warfare Strategy Implementation Plan Study* (Washington, DC: Center for Strategic and Budgetary Assessments, 2019). Available by request from OUSD (Acquisition & Sustainment).

the new Strategic Support Force (SSF). The creation of the SSF was one element of a larger military reform that established five new theater commands in place of the previous seven administrative military districts, differentiated the operational role of theater commanders from the training and equipping role of the PLA's military services, and reduced the size of PLA ground forces.[40]

The SSF comprises two departments. The Space Systems Department oversees nearly all aspects of PLA space operations, including satellite launch, tracking, telemetry, and space warfare. The Network Systems Department combines former PLA organizations responsible for cyber warfare, electronic warfare, psychological warfare, and information operations. The SSF conducts strategic information support, which consists of network operations and intelligence gathering and dissemination. More importantly for U.S. EMS operations, the SSF also conducts strategic information operations, which are designed to "paralyze the enemy's operational system-of-systems" and "sabotage the enemy's war command system-of-systems" during the early stages of a conflict.[41]

The creation of the SSF reflects the view of PLA leaders that the information environment will be the central battlefield of the future and that Integrated Network and Electronic Warfare (INEW) will be needed to succeed. Similar to the U.S. Army's recent adoption of the Cyber and Electromagnetic Activities (CEMA) operational construct, the PLA's decade-old concept of INEW describes how PLA EW and cyber units will comprehensively deny an adversary useful information in the EMS and cyberspace, including through deception and by herding communications onto compromised networks or frequencies. Unlike U.S. Cyber Command that solely focuses on cyber, the SSF includes space, cyber, and EW capabilities, and it is also responsible for organizing, training, and equipping strategic cyber and EW forces. Notably, however, the military services remain responsible for training and equipping operational- and tactical-level cyber and EW units; when deployed, these units are under the operational control of theater commanders. This seam between the SSF, military services, and theater commanders may present an opportunity for DoD.[42]

In conjunction with its organizational reforms, the PLA has embarked on an aggressive modernization program during the last three decades, including in capabilities for EW and EMSO. Consistent with its concept of Systems Destruction Warfare, the PLA has fielded a comprehensive set of jammers and other electronic countermeasures targeting U.S. sensors and communications as part of the PLA's information confrontation system. PLA EW systems are designed to suppress, degrade, disrupt, or deceive enemy electronic systems operating in

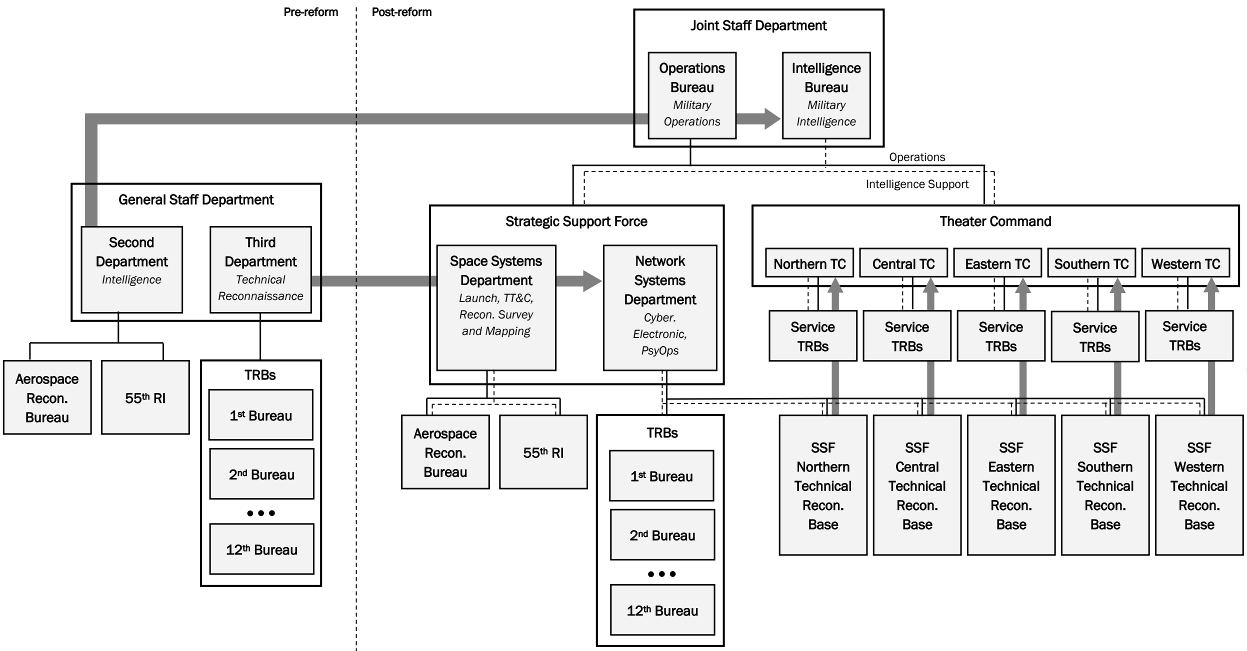
40 Christine Garafola, "People's Liberation Army Reforms and Their Ramifications," *The RAND Blog,* September 23, 2016.

41 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: National Defense University Press, 2018).

42 Ibid.

radio, radar, microwave, infrared, and optical frequency ranges, as well as adversary computer and information systems. China has also fielded several types of UAVs with EW payloads.[43]

FIGURE 7: ORGANIZATION OF THE SSF AND ITS PREDECESSOR ORGANIZATIONS



Costello and McReynolds, *China's Strategic Support Force*.

To find and engage U.S. and allied forces, the PLA deploys a wide array of passive and active sensors in its reconnaissance intelligence system and long-range precision cruise and ballistic missiles in its firepower strike system.[44] Although extensive, the relatively static structure of the PLA's SoS architecture may present opportunities for DoD to undermine the confidence of PLA commanders.

The PLA has begun to evaluate its EW and EMS capabilities operationally in force-on-force training events. These include the BLUE SHIELD air defense exercise, RED SWORD base-vs.-base exercise, HEAVENS SWORD strike exercise, and the LUOYANG exercise that pitted an SSF base against a combined force of ground, air, and rocket units. During exercises, PLA units regularly jam or confuse communications, sensors, and satellite navigation systems and conduct anti-jamming operations in support of PLA C4ISR.[45] Exercises have relied on PLA opposition forces using PLA equipment, but the tactics being used by opposition forces are unknown.

43 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 64.

44 Engstrom, *Systems Confrontation and System Destruction Warfare*, p. 25.

45 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, pp. 23, 64.

Russia

The Russian military has mounted a dramatic reform of its EW forces and capabilities since 2009. During the past decade, the Russian Armed Forces have modernized the equipment of 80 to 90 percent of its EW units. In support of Syrian government forces, Russian EW units are gaining operational experience through regular rotations to Syria where they jam GPS and communication systems of rebel forces and their U.S. allies.[46]

Russian EW personnel and equipment, or what Russian doctrine calls "assets," are organized into three main types of units:[47]

1. EW assets of military districts and the armed forces' services and arms;
2. EW assets in the KTK (Comprehensive Technical Control, a Russian term for passive EMS monitoring capabilities) system; and
3. EW assets of the strategic radio jamming system.

Most of the Russian military's EW systems and personnel are in the first category, distributed to Army EW brigades, Airborne EW companies, and individual ships and aircraft. The KTK system is a parallel organization within all EW units responsible for spectrum management and monitoring, emissions control (EMCON), and information assurance. The purpose of the strategic radio jamming system is not well understood, but is likely responsible for coordinating operations by EW forces in the services that impact nuclear and homeland defense communications and sensing.[48]

Although EW capabilities and operators are distributed throughout the Russian Armed Forces, they are largely organized into units of specialized EW troops operating stand-alone EW systems. Dedicated EW brigades in the Russian army operate alongside other functional brigades and are part of each division. On ships and in aircraft squadrons, EW personnel are organized into groups that operate UAVs and other stand-alone EW systems, rather than being incorporated into the ship or aircraft crew. The integrated EW equipment onboard ships and aircraft are generally less capable than the systems operated by their associated EW unit.[49]

EW personnel require a higher technical aptitude than other troops, particularly in the ground forces, which reduces the pool of potential recruits and qualified EW personnel. This

46 Madison Creery, "The Russian Edge in Electronic Warfare," *Georgetown Security Review*, June 26, 2019, available at https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/.

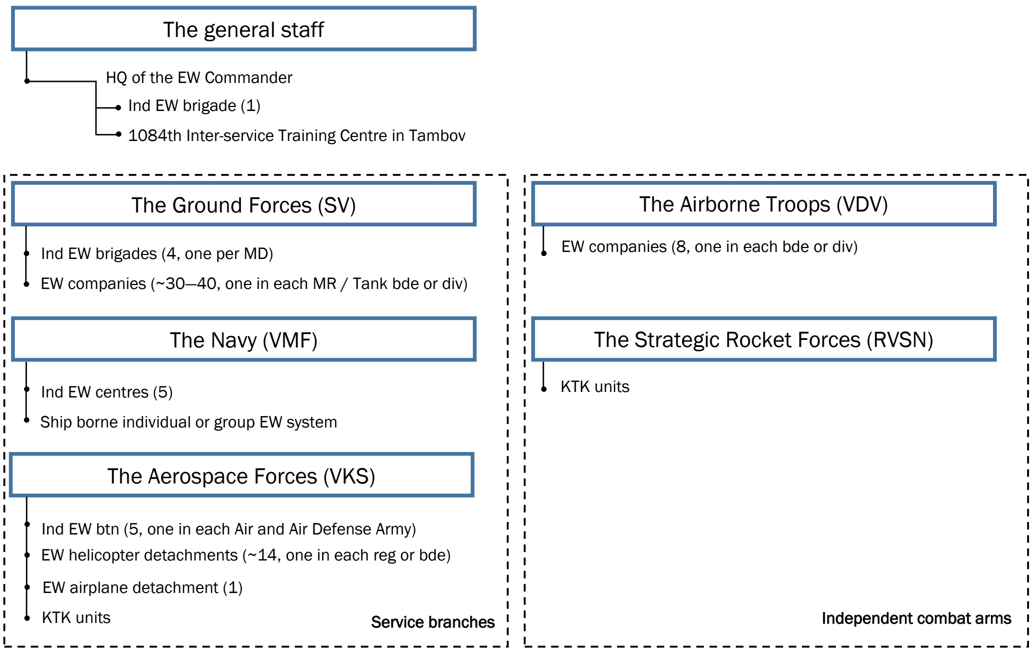
47 Jonas Kjellén, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces* (Stockholm: FOI, 2018), pp. 31–32, available at https://www.foi.se/rest-api/report/FOI-R--4625--SE.

48 Ibid.

49 Ibid., p. 33.

represents a longstanding shortfall in the Russian military.[50] As a result, a substantial portion of EW personnel are short-term conscripts, rather than longer-term contract servicemembers. Although the proportion of conscripts has decreased during the past decade from more than half to about one-quarter, this remains a challenge for the Russian Armed Forces because conscripts generally have shorter terms than contract personnel and are therefore less likely to become proficient at EW operations.

FIGURE 8: ORGANIZATION OF EW UNITS IN THE RUSSIAN ARMED FORCES



Kjellén, *Russian Electronic Warfare*, p. 34.

Although constrained by the number of new EW personnel, initial and recurring training for EW personnel has improved since the start of Russian Armed Force reforms in 2009.[51] All non-commissioned EW specialists are trained at the central training center at Tambov, and EW officers are trained at the Air Force Academy at Voronezh. Units receive regular retraining at their home station—or at Tambov when they receive new equipment. Some senior non-commissioned operators or officers also receive advanced training.

As noted above, Russian EW equipment is undergoing modernization, and about 70 percent of pre-2009 systems are projected to be replaced by 2020.[52] The Russian military services

50 Timothy L. Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015), p. 156.

51 Kjellén, *Russian Electronic Warfare*, p. 35.

52 Thomas, *Russia Military Strategy*, p. 153.

now field a wide variety of vehicle-borne jammers and passive sensors covering relevant radio frequency (RF) and visual spectra. Most of these systems are designed to perform a single function in a narrow frequency range. And although modernized, many of the new Russian EW systems are merely updated versions of Soviet technology. Furthermore, most aircraft and shipboard EW systems are for self-defense rather than delivering effects against enemy sensors or communications.

Russian EW units are fielding a small number of new technologies, including UAV-based jammers and sensors, precision-guided munition (PGM) jammers, and wide-area high frequency (HF) jammers. Russian EW units are also deploying EW command and control (C2) systems designed to coordinate planning and deconfliction of EW actions, but they are not intended to conduct autonomous, real-time spectrum management and control of EMS emissions like the EMBM systems being pursued by the U.S. military.[53]

United States

The U.S. military is generally behind those of Russia and China in modernizing its EW forces, although DoD has arguably developed the best EW and EMSO technologies of the three great power competitors. DoD's organizations and programs for EW and EMS operations can be assessed against the four goals of DoD's current EW Strategy.

Goal 1: Organize the EW enterprise to ensure EMS superiority. DoD established the EW EXCOMM and EMSO CFT to oversee and integrate the military Services' and combat support agencies' diverse efforts to improve their ability to gain and maintain EMS superiority. The EW EXCOMM's members and supporting personnel hold this as a collateral duty, whereas the EMSO CFT's members are full-time.[54]

The EW EXCOMM and EMSO CFT, however, lack the authorities or dedicated command structure of the Russian Armed Forces EW command or the PLA SSF, both of which establish requirements for EW doctrine and capability development and control most of their respective militaries' operating EW forces. All three militaries, however, have a diverse set of organizations responsible for developing and fielding EW and EMS capabilities. For DoD, these include four military Services and multiple agencies, including DARPA and the Missile Defense Agency (MDA).

As part of its organizational efforts, DoD has pursued professionalization of the EW and EMSO workforces. Within each of the military Services, enlisted personnel are coherently organized into EW and EMSO-related specialties and benefit from professional development programs throughout their careers. Officers, on the other hand, are often part of a larger

53 Kjellén, *Russian Electronic Warfare*, p. 62; Clark and McNamara, *Electronic Warfare Strategy Implementation Plan Study*, p. 42. Available by request from OUSD (Acquisition & Sustainment).

54 DoD, "Electronic Warfare Policy," DoD Directive 3222.04, Change 1, May 10, 2017, p. 2; and Shanahan, "Establishment of the EMS Operations Functional Team," p. 2.

community such as aviation or combat systems and only lead EW or EMS operations as a collateral duty. Officers in dedicated EW or EMSO career fields such as communications, Navy or Air Force airborne EW, and Army CEMA usually only perform these duties during their first few operational tours and spend the rest of their time participating in graduate education, other missions, or acting as senior leaders and managers.[55]

Goal 2: Train and educate forces for 21st Century EW and EMS operations. In DoD, EW and EMSO training is delegated to military Services and agencies, leading to uneven progress of training improvements. The U.S. Navy, Marine Corps, and Army have all, to varying degrees, incorporated EMSO training into their basic and general military training for all personnel, and the U.S. Air Force is developing a training program for all airmen.

Training for EW personnel has been more varied. Each Service's enlisted and officer EW or EMSO community has well-developed initial training and qualification programs. Advanced training is provided to enlisted personnel as part of their professional development processes, whereas officers receive less follow-on EW or EMSO training because they generally are part of a larger non-EW or EMSO community.

At the unit level, practical training for U.S. EW or EMSO-focused organizations requires improvement. Home stations across DoD lack adequate facilities for live or simulated training on EW and EMS operations. Units are often limited to classroom or computer-based academic training to maintain proficiency between major pre-deployment training events or certification exercises at combat training centers (CTC).[56] The lack of unit training often requires EW and EMSO organizations to receive remedial instruction at CTCs before proceeding with the planned exercise.

Facilities at CTCs generally do not include the most advanced threat capabilities, but DoD is improving at employing dedicated opposition forces (OPFOR) to test U.S. EW and EMSO units. CTC facilities are also unable to test all aspects of U.S. EW and EMSO operations. For example, U.S. Air Force and Navy aviation units can practice offensive EW and EMSO against air defense systems and communication networks at training ranges, but ships are limited to practicing defensive EMCON operations or, occasionally, self-protection jamming. The U.S. Army and Marine Corps are quickly improving their ability to test ground units at CTCs in both offensive and defensive EW and EMS operations.

Home station and CTC training could be improved through a new approach to live, virtual, and constructive (LVC) training that upgrades facilities for virtual and constructive training instead of modernizing live training ranges. Because virtual and constructive training systems can be affordably scaled once developed, they could be used at home stations and CTCs. This

55 See Clark and McNamara, *Electronic Warfare Strategy Implementation Plan Study*, p. 8. Available by request from OUSD (Acquisition & Sustainment).

56 Such centers include the Virginia Capes exercise area for the U.S. Navy or Nellis Training and Test Facility, NV for the U.S. Air Force.

approach would also address growing operational security (OPSEC) concerns regarding open-air training against advanced threats at CTC ranges.

Goal 3: Equip the force with agile, adaptive, and integrated EW capabilities. DoD and the U.S. defense industry are at the leading edge in developing new EW and EMSO technologies, particularly adaptive, cognitive, and multifunction EW and EMS systems. DoD has been challenged, however, to transition these new technologies into acquisition programs due to the inability of the U.S. military's requirements development process to generate demands for new technologies. For example, because cognitive EW and EMSO systems are designed to address unknown or unexpected situations and signals, they do not service existing gaps revealed by DoD's Joint Capabilities Integration and Development System (JCIDS). Multifunction EW and EMS systems could address requirements for several different existing programs, but for some programs the new capability would be ahead of need. And even if requirements could be agreed to, acquisition of multifunction systems would necessitate integrating efforts and funding from several disparate program offices and sponsors.

DoD is improving its ability to introduce new EW and EMSO technologies into acquisition programs, as evidenced by the incorporation of adaptive EW algorithms into several new defensive and offensive EW systems, which could evolve into cognitive EW systems.[57] Furthermore, recent changes in acquisition law and policy have allowed DoD to begin fielding new multifunction EW capabilities.[58]

Networked EW capabilities are farther behind DoD cognitive, adaptive, and multifunction EW and EMS technologies. Some small-scale, tailored networked EW systems have been fielded, but larger, ad-hoc networked EW capabilities have not been developed. This is largely due to challenges facing EMBM systems development, to include modeling and simulation, data standard and communication system compatibility, and algorithms for distributed control of EW and EMS operations among multiple systems or platforms. Some Service-developed EW and EMSO management systems, such as the U.S. Army EW Planning and Management Tool (EWPMT) or the U.S. Navy's Real-Time Spectrum Operations (RTSO) system, may provide a useful starting point for a joint networked EW capability.[59]

Emerging adaptive, cognitive, multifunction, and networked EW and EMSO technologies are driving the necessity for ES capabilities to be incorporated into every system operating in the EMS. U.S. forces will increasingly need to reduce or eliminate their active emissions and find enemy targets using passive geolocation, passive radar, or other covert techniques provided through ES. ES could also enable more capable low-probability of intercept/low probability of

57 Mark Pomerleau, "AFRL Seeks Cognitive Electronic Warfare Research," *C4ISRNet,* July 11, 2016.

58 Ellen Lord, Under Secretary of Defense "Middle Tier of Acquisition (Rapid Prototyping/Rapid Fielding) Interim Governance," memorandum, October 9, 2018, available at https://www.dau.edu/policy/PolicyDocuments/Middle-Tier-of-Acquisition-Interim-Governance.pdf; and Mark Pomerleau, "How Redefining Army Intel Can Help Fight High-End Adversaries," *C4ISRNet,* May 24, 2018.

59 Sydney J. Freedberg Jr., "Army Boosts Electronic Warfare Numbers, Training, Role," *Breaking Defense,* August 7, 2018.

detection (LPI/LPD) communication and radar systems by finding and identifying potential enemy jammers or receivers. DoD is increasing its incorporation of ES capabilities into EW and EMSO systems, but more improvements will be needed to enable the next generation of EW and EMSO technologies to be fully realized.

Goal 4: Bolster partnerships with industry, academia, interagency and allied partners. Through professional organizations and new consortia, DoD has strengthened its partnerships with industry and academia. DoD's efforts to improve integration with allies are more uneven. DoD has a robust EW and EMSO relationship with North Atlantic Treaty Organization (NATO) allies through the NATO Electronic Warfare Advisory Committee (NEWAC) and Conference of National Armaments Directors (CNAD). The NEWAC is responsible for development of requirements and oversees NATO's EW policy, doctrine, and C2 concepts, and it oversees EW support to NATO operations and exercises. The CNAD oversees acquisition policy and interoperability. Interoperability with NATO is becoming more difficult, however, with the introduction of new cognitive and networked U.S. EW and EMSO capabilities, which are not being introduced in other NATO militaries.

DoD's EW and EMSO relationship with Australia is strong; it is bolstered by the sale of U.S. E/A-18G Growler airborne electronic attack (AEA) aircraft to the Royal Australian Air Force (RAAF) and frequent technical exchanges between U.S. and Australian Defense Force (ADF) personnel. Australian companies such as CEA are also potential providers of EM systems to DoD.

By contrast, DoD's relationship with Japan, an essential ally in the competition with China, is not strong regarding EW and EMSO. Due to concerns with Japan's industrial security program, DoD generally does not share EW or EMSO technologies with Japanese industry, which lacks robust indigenous EW or EMSO R&D programs. The lack of R&D and a paucity of new EW and EMSO concepts and requirements from the Japan Self Defense Force (JSDF) has slowed introduction of new EM technologies into the JSDF. This limits the ability of DoD and the Japan MoD to coordinate EW or EMSO requirements and capability development between their militaries.[60]

Asymmetries

Significant divergences between the EW and EMSO strategies, concepts, and capabilities of the U.S. military and those of China and Russia can reveal challenges and opportunities for DoD in its pursuit of EMS superiority. Rather than conducting a gap analysis to identify where U.S. forces will fall short in pursuing their desired tactics against a specific threat in a particular set of situations, this analysis highlights challenges and opportunities based on enduring

60 See Clark and McNamara, *Electronic Warfare Strategy Implementation Plan Study*, p. 42. Available by request from OUSD (Acquisition & Sustainment).

strengths and weaknesses that are less sensitive to changing circumstances—and that are likely to endure beyond a single budget cycle.

Analysis of fundamental asymmetries in a mission area can also suggest areas where DoD either cannot gain an advantage or cannot do so affordably and in a reasonable period of time. Further investment in these areas may not be beneficial. Asymmetries can also show where areas that appear at first to be a challenge, but that can be turned into a potential opportunity and advantage. Other asymmetries are already areas of advantage that should be enhanced through DoD efforts.

The major asymmetries between the U.S., Chinese, and Russian militaries with regard to EW and EMSO are detailed below, followed by their implications for DoD. The recommendations arising from this analysis are discussed in the following chapter.

Counter-intervention vs. power projection strategies

The PLA and Russian Armed Forces have adopted strategies that focus on hindering or preventing intervention by U.S. military forces in the Western Pacific and Eastern Europe, respectively, and are supported by extensive networks of long-range sensors and weapons.[61] These strategies emerge from the nature of Chinese and Russian national security interests, which center on maintaining or expanding territory and influence along their countries' peripheries. If or when the Chinese or Russian governments pursue national security objectives farther abroad, their militaries would need to rebalance toward expeditionary and power projection capabilities of their own. China's most recent defense white paper suggests the PRC government is shifting its focus toward protection of Chinese interests abroad, but its investments and posture continue to reflect an emphasis on near seas defense.[62]

Chinese and Russian military strategies differ considerably from the U.S. emphasis on power projection to stop or retaliate against aggression.[63] The asymmetry between U.S. and competitor strategies, and their supporting military capabilities, sets up a contest between the American strategic offense and Chinese or Russian strategic defense, one in which the United States must contend with the tyranny of distance as the "away team." The United States has traditionally dealt with this imbalance by using alliances, forward posture, and improved protection schemes to make itself a stronger incumbent force in the Western Pacific

61 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 15; DIA, *Russia Military Power*, pp. 23, 32.

62 Andrew Erickson, "China's Defense White Paper Means Only One Thing: Trouble Ahead," *The National Interest,* July 29, 2019. The PLAN continues to field a larger number of frigates, corvettes, and non-nuclear submarines suited for coastal and littoral missions and has not developed a sizable fleet of aerial refueling, logistics ships, and large surface combatants needed for power projection operations overseas. See Bryan Clark and Jordan Wilson, "Competition in the Maritime Realm," in Tai Ming Cheung and Thomas G. Mahnken, eds., *The Gathering Pacific Storm: Emerging US-China Strategic Competition in Defense Technological and Industrial Development* (Amherst, NY: Cambria Press, 2018).

63 Mattis, *Summary of the 2018 National Defense Strategy*, p. 7; and Chris Dougherty, *Why America Needs a New Way of War* (Washington, DC: Center for a New American Security, 2018), p.7.

and Eastern Europe, placing the United States and its allies on the strategic defense as well.[64] DoD could continue this approach and enhance it through new EW and EMSO concepts and capabilities.

SoS architectures vs. kill webs and mission command

Military force design and C2 concepts are necessarily interrelated. For example, a force operating close to home on the strategic defense can rely on interior lines of communication and employ a relatively static force design and centralized command relationships. An expeditionary force, on the other hand, will require a more flexible design and more independent decision-making by field commanders.

The asymmetry is reflected in the force design and C2 processes of the Chinese, Russian, and U.S. militaries. The PLA employs an integrated collection of SoSs designed to paralyze opposing forces' C2 and ability to deliver effects, rather than annihilating the enemy through attrition.[65] This approach, which Chinese military strategists describe as Systems Warfare or System Destruction Warfare, leverages the PLA's knowledge of where conflict is likely to occur, the PLA forces to be employed, and the likely variety of enemy dispositions and tactics. System Destruction Warfare seeks to exploit perceived vulnerabilities of the U.S. military, such as its reliance on communications links and active monostatic radars. The PLA's SoS-centered force design is intended to provide redundancy and robustness, but may do so at the expense of flexibility and resilience. Although the force-wide SoS may be assembled during the lead-up to conflict, the component SoS and systems were designed well in advance to address the likely range of operational situations and U.S. material and operational responses.[66]

The U.S. force design approach also relies on SoS architectures, but is the outgrowth of a much different organizational culture and historical experience from that of either China or Russia. As an expeditionary force, the U.S. military is less able to construct a highly redundant and resilient SoS force structure. The locations, opponents, allies, and U.S. forces available for future conflicts are unknown, requiring a force design with the flexibility to accommodate a wider variety of force compositions than would be necessary for a "home team" military like the PLA. Current U.S. military leaders sometimes characterize this approach as a "kill web" rather than the traditional kill chain.[67]

64 See, for example, Thomas G. Mahnken, "U.S. Strategy: Confronting Challenges Abroad and Constraints at Home," in Ashley J. Tellis, Alison Szalwinski, and Michael Wills, eds., *Strategic Asia 2017–18: Power, Ideas, and Military Strategy in the Asia-Pacific* (Seattle, WA and Washington, DC: National Bureau of Asian Research, 2017).

65 Kevin McCauley, *PLA System of Systems Operations: Enabling Joint Operations* (Washington, DC: Jamestown Institution, 2015).

66 Engstrom, *Systems Confrontation and System Destruction*, pp. 19-21.

67 Megan Eckstein, "Interview: Rear Adm. Mike Manazir on Weaving the Navy's New Kill Webs," *USNI News,* October 3, 2016.

The Russian Armed Forces reflect elements in common with PLA and U.S. force designs. The Russian military attempts to create a static and robust EW and EMSO SoS in important regions such as the Western Military District adjacent to Belarus and the NATO Baltic states. During their expeditionary operations in Syria and Ukraine, Russian forces rely on networked mobile EW and EMSO systems to win information confrontations. In both homeland and expeditionary contexts, however, the coordination and integration of Russian EW and EMSO capabilities falls short of the PLA or DoD, respectively.[68]

The C2 approaches employed by the PLA and Russian Armed Forces reflect a scientific view of warfare. Under the concept of System Destruction Warfare, PLA C2 relies on tactics analyzed and agreed to in advance by consensus and implemented through pre-architected SoS for C2, fires, reconnaissance, and intelligence.[69] The Russian C2 approach delegates authority to subordinates but values the ability to exercise systemology, a Russian theory of combat systems that relies on modeling and cybernetics, to scientifically command forces and anticipate combat outcomes.[70] These C2 concepts are quite different from those of the U.S. military, which delegate authority to subordinates and rely on a junior leader's judgment and ability to follow the commander's intent in situation when communications are lost with senior leaders. This approach is characterized in U.S. military doctrine as "mission command."[71]

A significant limitation of mission command is the lack of planning and management tools available to junior commanders. As a result, they are likely to fall back on habit or doctrine, making their actions more predictable and losing much of the value in mission command. This challenge will only grow as the DoD adopts more distributed force architectures involving larger number of unmanned systems under operational concepts such as Multi-Domain Operations (MDO) or Distributed Maritime Operations (DMO).[72] If junior commanders had better planning and management tools, they may be able to improvise more effectively, possibly invalidating assumptions built into PLA SoS architectures.[73]

One approach is not necessarily better than the other. Pre-planned and architected operations trade flexibility for more robust analysis of potential opportunities and challenges; delegation and mission command give up extensive tactics development in the hope that innovation and

68 Glen E. Howard and Matthew Czekaj, eds., *Russia's Military Strategy and Doctrine* (Washington, DC: Jamestown Foundation, 2019), pp. 308–309.

69 Engstrom, *Systems Confrontation and System Destruction Warfare*, pp. 25–43; and DIA, *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: DIA, 2018), p. 25.

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

71 Douglas M. McBride Jr. and Reginald L. Snell, "Applying Mission Command to Overcome Challenges," *Army Sustainment,* January–February 2017, available at https://www.army.mil/article/179942/applying_mission_command_to_overcome_challenges.

72 U.S. Army Training and Doctrine Command (TRADOC), *The Army in Multi-Domain Operations 2028* (Ft. Eustis, VA: TRADOC, December 6, 2018), pp. 32–44, available at https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

73 Mark Pomerleau, "DARPA Multidomain Program to Focus on 'Kill Webs'," *C4ISRNET*, May 10, 2018.

creativity will overcome obstacles—or at least confuse the enemy. If U.S. commanders were provided more capable planning tools and the training to employ them, these tradeoffs may no longer apply. A junior commander could execute previously unconsidered tactics and force compositions while gaining many of the potential benefits of pre-planned operations.

Specialization vs. flexibility

The PLA and Russian Armed Forces field a wide variety of EW systems that are mostly designed to address certain types of adversary capabilities or even specific systems. Chinese and Russian EW systems and personnel are organized into specialized EW units, and those units are dispersed during operations to work alongside fires, C4ISR, and maneuver formations. As a result, the PLA and Russian Armed Forces deploy significant EW and EMSO capacity. The plethora of EW systems employed by Chinese and Russian forces and their variety of underlying technologies may constrain the ability of PLA and Russian Armed Forces units to broadly adopt new technologies such as adaptive or cognitive EW, networked EW, and EMBM.

U.S. EW capabilities are also organized into specialized EW units for training and administrative purposes and dispersed to integrated formations for preparation and deployment.[74] U.S. forces employ a much smaller diversity of EW platforms and systems compared to Russian and Chinese militaries, but these systems tend to be more multifunctional and are designed to individually address a wider range of threats. The narrower diversity of U.S. EW and EMSO systems may enable the U.S. military to more easily field new EW and EMSO technologies than their Chinese or Russian counterparts. For example, U.S. EW and EMSO units are already incorporating AI and ML-enabled algorithms into operational airborne EW systems and fielding networked EW capabilities into shipboard and land-based EW and EMSO systems.[75]

EW vs. EMBM

As part of their counter-intervention strategies, the Chinese and Russian militaries seek to use EW to degrade or deceive U.S. and allied radars, satellite navigation, and communications; EW often includes passive RF sensors to enable attacks on opposing C2 systems by finding and targeting emitters like radios and radars. The Chinese and Russian militaries also consider EW as part of a unified effort with cyber operations to control and manipulate the

74 Doni Wong, Theodore Lipsky, Brigid Calhoun, and Pablo Cruz, "Integration of Signals Intelligence, Electronic Warfare in Reconnaissance Troop: Seeing Where the Eye Cannot See," *ARMOR*, Fall 2018, available at https://www.benning.army.mil/Armor/eARMOR/content/issues/2018/Fall/4Wong18.pdf.

75 DoD, "Integrated Defensive Electronic Countermeasures (IDECM)," Selected Acquisition Report (SAR), Defense Acquisition Management Information Retrieval, December 2017, available at https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/18-F-1016_DOC_60_Navy_IDECM_SAR_Dec_2017.pdf.

information available to an opponent; the PLA characterizes cyber-EW integration as INEW, whereas the Russian Armed Forces call it information confrontation.[76]

Because their potential military objectives are nearby, the PLA and Russian Armed Forces can base most of their EW and sensor systems on their own territory, where they can rely on wired communications, or in nearby sea or airspace, where line-of-sight RF communications will be reliable and difficult to jam. The Chinese and Russian militaries can therefore pre-plan their spectrum use and do not need to coordinate EW operations, sensing, and communications in real time. As an expeditionary force, the U.S. military expects to manage the spectrum dynamically and integrate different actions in the EMS through concepts like JEMSO and by using EMBM systems. While DoD is pursuing several systems to achieve this, it has not yet fielded any.[77]

Passive vs. active sensing

By establishing military objectives in proximity to their own territory, the Chinese and Russian governments have enabled the PLA and Russian Armed Forces to emplace sensor networks that cover the area in which future military operations would be likely to occur, as well as the air, maritime, and land approaches that intervening U.S. forces would use to aid a beleaguered ally. Control of the territory on which sensors are established allows the PLA and Russian Armed Forces to employ techniques such as passive RF detection and geolocation or HF radars that employ multiple antennae to obtain views from a variety of aspects, large arrays to obtain higher gain, and a deep understanding of the local electromagnetic and physical environment. Although they require more infrastructure, these techniques can achieve longer detection ranges than higher-frequency shipboard or airborne radars and, if passive, can avoid revealing the sensor's nature and location.

The passive sensors and HF radars the PLA and Russian Armed Forces employ create a significant asymmetry with expeditionary U.S. and allied militaries. Because they are mobile, platform-centric, and often not resident in the region, U.S. and allied forces are less able to employ sensor techniques requiring large or multiple stationary arrays. U.S. ships, aircraft, maneuver forces, and forward posts and bases often rely on active, monostatic radars for situational awareness and defense. Furthermore, expeditionary U.S. and allied forces are dependent on EMS communications to coordinate operations, whereas Chinese and Russian sensor network can rely on wired communications.

DoD has little ability to change Chinese or Russian security objectives or the U.S. military's fundamental need to project power in most likely future confrontations. The U.S. military could, however, adjust its operational concepts and capabilities to reduce its vulnerability to

76 DIA, *Russia Military Power*, p.42; OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 64; and Costello and McReynolds, *China's Strategic Support Force: A Force for a New Era*, p. 7.

77 Sydney J. Freedberg Jr., "Managing The Chaos Of Electronic Warfare," *Breaking Defense,* October 8, 2014; and Jill Atoro, "Is Electronic Warfare Already Legacy Technology?," *C4ISRNET,* June 7, 2019.

detection and tracking by degrading the ability of opposing forces to understand the disposition and intent of U.S. forces.

Experimentation vs. deliberate planning

The Russian and, to a lesser degree, Chinese militaries conduct more frequent and extensive EW experimentation compared to the U.S. military. This is in part a function of their having more numerous and diverse EW systems than those fielded by DoD. But it is also because the Chinese and particularly Russian militaries have greater opportunities to experiment. The Russian Armed Forces leverage current operations in Syria and Ukraine, whereas the PLA has an extensive range architecture to support EW system test and experimentation.[78]

Chinese and Russian EW experimentation efforts also reflect their respective C2 approaches. The PLA pursues experimentation as part of its process of deliberate system and concept development, which will produce a consensus on the best combination of systems and tactics to employ in expected situations. The Russian military's willingness to delegate command and rely on subordinates' creativity contributes to its willingness to experiment during actual operations. The results and insights from experimentation are then shared among the rest of the force.

In contrast to frequent and dedicated Chinese or Russian experimentation, DoD does not pursue extensive EW or EMS experimentation due to concerns about operational security and access to ranges and other appropriate instrumented facilities. As a result, the U.S. military predominantly conducts experimentation during demonstrations that seek to prove the viability of a new technology or force-on-force exercises that also have training, evaluation, and certification objectives. The competing goals of U.S. exercises and demonstrations could reduce their value as opportunities for pure experimentation and concept development. An increased reliance on virtual and constructive systems for EW and EMSO training could improve DoD's ability to experiment, as could a new approach to R&D that combines technical and operational innovation.

Officer vs. senior enlisted technical management in EW and EMSO

The PLA and Russian Armed Forces rely on officers from military academies and a combination of contract and conscript enlisted personnel to operate and maintain EW and EMS operations systems. Chinese and Russian EW and EMO officers receive extensive technical training and spend most of their career in the field. This compensates for relatively short enlisted careers, which range from 2-year conscription to 4-year contracts. Enlisted personnel in the PLA and Russian Armed Forces do not generally remain in the military for multiple

78 Mark Pomerleau, "Why Syria May Be the most Aggressive Electronic Warfare Environment on Earth," *C4ISRNet,* April 24, 2018; and OSD, *Military and Security Developments Involving the People's Republic of China 2019.*

contracts because both militaries rely on officers for technical management, and there are few positions for senior enlisted leaders.[79]

The balance between officer and enlisted technical leadership is essentially reversed in the U.S military, where from one-third to one-half of enlisted personnel stay for multiple contracts, and many complete a 20- to 30-year career. U.S. officers overseeing or conducting EW or EMSO operations receive a few months to a year of training, but usually only perform EW or EMSO duties for one or two tours of 3 years each during a 20-year or longer career.

The Russian and Chinese militaries' lack of a corps of senior enlisted technical experts does not necessarily degrade their operational capability. Their junior enlisted personnel receive as much training as their U.S. counterparts, and PLA or Russian Armed Forces EW officers are in general more highly trained and more experienced than U.S. officers.

Civil-military fusion vs. military R&D

The Chinese and, to a lesser degree, Russian governments practice civil-military fusion or integration, in which technical advancements developed in the commercial sector are accessible to or are supported by the military R&D enterprise.[80] This dramatically expands the government and military's research and industrial base and may allow the Chinese or Russian governments to access commercial technology a private company is developing in concert with an American or European organization. U.S. and European companies are not required to share or contribute ideas and technology to their respective governments, and often resist government efforts to buy or co-develop technology.[81]

The asymmetry between the R&D activity and intellectual capital available to the U.S. military compared with China and Russia arguably hinders DoD's ability to adopt and exploit new technologies. Another interpretation, however, could be that commercial innovation may be stifled in Russia and China by intervention of the government in private R&D. The U.S. and European approach of unfettered innovation within a regulatory framework may foster the development of more numerous and disruptive technologies and concepts. This potential advantage, however, is often lost to DoD because of its inability to quickly adopt new technologies and transition them into operational use. A new approach to R&D that focuses less on the opportunities a new technology may provide rather than its ability to fill an existing gap could alleviate the U.S. disadvantage.

79 Kjellén, *Russian Electronic Warfare*, p.34; and OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 61.

80 Lorand Laskai, "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise," *Council on Foreign Relations blog,* January 29, 2018; and OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 31.

81 Zak Doffman, "Google Accused by Top U.S. General and Senator of Supporting Chinese Instead of U.S. Military," *Forbes*, March 16, 2019.

Allies vs. clients

The United States is party to seven multilateral and bilateral mutual defense alliances.[82] To Russia's west in Europe, the U.S. military is the bulwark and largest force within NATO. NATO increasingly recognizes the political and military challenge posed by Russia and is improving the alliance's posture and defensive capabilities.[83] U.S. forces are permanently stationed at several NATO bases in central and western Europe and are increasing their permanent presence in Eastern Europe.[84] To Russia's east, Japan also faces a more revisionist Russian foreign policy and interdicts frequent Russian Air Force intrusions into Japanese airspace.[85]

The U.S.-Japan alliance is also relevant to the global U.S.-China strategic competition and the intensifying competition between China and Japan in the East China Sea. In response to these tensions, the Japanese government is modernizing and growing the JSDF, as well as expanding into new capability areas such as amphibious operations. For its apart, DoD is growing the number and capability of U.S. forces based in Japan, adding ships and replacing legacy aircraft with 5th generation F-35 strike-fighters.[86] The United States is also allied with the Philippines, Thailand, the Republic of Korea, New Zealand, and Australia. Although the more than 20,000 U.S. troops permanently based in South Korea are largely dedicated to deterring and responding to North Korean aggression, U.S. forces that rotate through facilities and military bases in the Philippines and Australia can help deter or respond to Chinese military or paramilitary actions.

Compared to the United States, China and Russia have few allies. China is allied with North Korea under the Sino-North Korean Mutual Aid and Cooperation Friendship Treaty, and Russia is allied with Armenia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan under the Collective Security Treaty Organization. Those allies they do have are more accurately described as client states, which provide military basing or access in return for Chinese or Russian investment or defense guarantees. Chinese and Russian client states are not expected to provide military assistance to PLA or Russian Armed Force units and are themselves unlikely targets for aggression, rendering them less in need of Chinese or Russian defense. The asymmetry in number and character between U.S. and Chinese or Russian alliances creates a significant opportunity for DoD to gain an advantage in the EW and EMSO competition, but the U.S. military has been slow to exploit the benefits of its alliances outside of conflict.

---

82 U.S. Department of State, "U.S. Collective Defense Arrangements," available at https://2009-2017.state.gov/s/l/treaty/collectivedefense/.

83 Julian Barnes, "NATO Considers Missile Defense Upgrade, Risking Further Tensions With Russia," *The New York Times,* July 5, 2019.

84 "Poland, U.S. Agree on Six Locations for U.S. Troops in Poland—Minister," *Reuters*, August 30, 2019.

85 Franz-Stefan Gady, "Japan Scrambles Fighter Jets 999 Times in 2018 in Response to Foreign Aircraft," *The Diplomat*, May 2, 2019.

86 Megan Eckstein, "Navy Adding Fifth Amphib to Japan-Based Fleet for Operational Flexibility; 1 DDG Leaving Japan," *USNI News*, April 29, 2019.

Joint vs. whole of government or society

Although U.S. mid-grade officers often note the lack of coordination or integration among U.S. military Services, U.S. operations are generally much more joint and multidomain than those of the PLA or Russian Armed Forces. Russian military leaders have not noted this is a significant problem for their forces, due to the predominant role of the Army and land operations and lack of overseas ambitions in Russian defense strategy and planning.[87] PLA leaders, on the other hand, have argued the Chinese military needs to better integrate operations across services and between domains. The PLA reorganization that started in 2015 was intended, in part, to improve "jointness" and promote cross-domain operations by establishing the SSF and creating joint theater operational commands instead of Army-dominated military district commands.[88]

Although their operations are less joint and integrated than those of the U.S. military, the PLA and Russian Armed Forces benefit from being part of more unified government or society-wide national security activities. The PRC government's mandate for civil-military fusion and centralized authority in the Central Military Commission (CMC) focuses commercial and government civilian activity on national security objectives at home and abroad.[89] For example, the combined efforts of the civilian People's Maritime Militia, governmental China Coast Guard, and military PLA Navy (PLAN) to prevent access to islands and features in the East and South China Seas promotes the CMC's goal of regaining control of disputed maritime territories.[90] In Russia, there is less formal integration between government agencies as well as between government and commercial entities. The Russian government relies on informal relationships among leaders, or oligarchs, who regularly move between the commercial and government to coordinate activities.

The United States has a much more disparate and less-integrated approach to pursuing national security interests. Coordination among agencies within the U.S. government is conducted through myriad cross-functional and interagency teams, as well as in senior-level integration groups such as the National Security Council (NSC) staff. Coordination between the U.S. government and commercial organizations is constrained by adherence to free-market principles, conflict-of-interest regulations, and sometimes by a company's resistance to cooperating due to policy disagreements with the U.S. government. The U.S. government

87 Michael Kofman, "It's Time To Talk About A2/AD: Rethinking the Russian Military Challenge," *War on the Rocks,* September 5, 2019, available at https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/.

88 Yasuyuki Sugiura, "The Joint Operation Structure of the Chinese People's Liberation Army with Focus on the Reorganization of the Chain of Command and Control under the Xi Jinping Administration," *NIDS Security Studies* 19, no. 1, March 2017, available at http://www.nids.mod.go.jp/english/publication/kiyo/pdf/2017/bulletin_e2017_2.pdf.

89 White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World* (Washington, DC: The White House, June 2018), p. 14, available at https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf; and OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 31.

90 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 79.

and military, however, continue to successfully partner with non-profit service and support organizations such as Project Hope or the Red Cross.

The Chinese and Russian militaries are better positioned to leverage coordination with other government and commercial organizations compared to the U.S. military, but this may prove to be a diminishing area of advantage for the PLA and Russian Armed Forces if commercial efforts are increasingly constrained to perceived government needs and independent R&D and discovery is not allowed to occur.

Implications for DoD EW and EMSO Strategy and Programs

An assessment of the above asymmetries in U.S., Chinese, and Russian EW and EMSO doctrine and trends reveal several categories of insights:

- Challenges DoD should acknowledge and attempt to mitigate;
- Challenges DoD should attempt to alleviate or overcome;
- Challenges that could be turned to opportunities; and
- Opportunities DoD should more fully exploit.

The asymmetries falling into these categories are discussed briefly below. The recommendations that follow from these implications are detailed in Chapter 3.

Challenges DoD should acknowledge and attempt to mitigate. Some asymmetries are nearly insurmountable. As a result, DoD should focus on mitigating their impact rather than solving them. For example, DoD cannot influence the ability of Chinese and Russian governments to integrate government and commercial activity toward national security objectives, nor can it change the ability of the PLA and Russian Armed Forces to focus on regional counter-intervention strategies and capabilities rather than power projection. It may, however, be able to reduce the impact of these asymmetries through new approaches to U.S. defense innovation or by challenging Chinese and Russian EMS superiority in areas outside their primary regions of military concern.

Challenges DoD should attempt to alleviate or overcome. Other challenges could be alleviated, such as the greater emphasis the Chinese and Russian militaries place on experimentation compared to the U.S. military or the ability of Chinese and Russian forces to employ passive and lower frequency active EMS sensors around their periphery. A shift by DoD away from live training and certification and toward virtual and constructive training could level the playing field in terms of experimentation and concept development. Adopting EMSO concepts and tactics that privilege passive, commercial, and LPI/LPD capabilities could reduce the threat from passive and lower-frequency active sensing.

Challenges that could be turned to opportunities. Some asymmetries would normally lead to a disadvantage for the U.S. military, but could be turned into an advantage through new concept and capability development priorities. For example, the larger number and variety of Chinese and Russian EW and EMSO systems compared to the U.S. military translates into a growing number of capability gaps. Instead of filling these gaps with new or modified systems, DoD could accelerate the development and fielding of adaptive or cognitive multifunction capabilities in new or existing EMSO systems and begin experimenting with the EMBM capabilities being developed in the Services. By decoupling EMSO systems from specific function, technique, or frequency ranges, DoD could reduce its own EMBM challenges while turning the variety and number of EW and EMSO systems in the Chinese and Russian militaries into an EMBM and sustainment liability. Another example of a challenge that could be turned to an opportunity is the Chinese military's reliance on a comprehensive SoS architecture to defeat U.S. forces by attacking U.S C4ISR capabilities. The PLA's ability to focus on counter-intervention could make this SoS approach more effective. The U.S. military could turn the PLA's relatively static SoS into a disadvantage, however, if U.S forces were to mount highly distributed and agile operations using recomposable units and AI-enabled planning and management tools.

Opportunities DoD should more fully exploit. A final set of asymmetries create opportunities that are clear today, but which DoD has not fully exploited. For example, U.S. forces could leverage the proximity of allies to conduct EW against Chinese and Russian forces in peacetime and support resilient EMSO during conflict.

Conclusion

DoD is unlikely to have the time or resources to identify and mitigate each individual gap in the U.S. military's ability to conduct EW and EMSO against Chinese and Russian forces using today's operating concepts and tactics. Instead, DoD should focus its efforts on the asymmetries that are likely to provide it a distinct and potentially enduring advantage, and accept the near-term shortfalls that may emerge. The following chapter will describe the actions DoD should take to exploit these opportunities.

CHAPTER 3

Recommendations and Conclusion

Several recent analyses and this assessment have found that DoD is falling behind its great power competitors in EW and EMSO.[91] The solution proposed by most evaluations, particularly those conducted by the U.S. government, is for DoD to dramatically increase spending on EW capabilities to fill gaps created by improving adversary countermeasures as well as develop new systems to hold opponents' emerging EMS capabilities at risk.[92]

Absent a strategy for how DoD will operate and fight in the EMS, however, more funding is unlikely to restore the ability of U.S. forces to gain and maintain EMS superiority. While spending on EW and EMSO grew over the last five years, DoD did not focus its resources on the most important new technologies and programs needed to gain an advantage in the EMS. The misapplication of funding continues into the Future Year's Defense Plan, as funding for development of new capabilities is planned to decrease while spending on procurement is projected to go mainly to upgraded versions of today's EW and EMSO systems.[93]

At the current incremental pace of EW and EMSO concept and capability improvement, DoD will need a decade or more to address its EMS capability gaps relative to the Chinese and Russian militaries. The U.S. government's fiscal constraints and the intensifying nature of today's competition with China and Russia may not afford the time for this approach to eventually bear fruit. Before the U.S. military is able to gain an advantage, the Chinese or Russian governments could be encouraged by shifting military balances, including those in the EMS domain, to pursue their military objectives through gray-zone operations, political warfare, or military aggression.

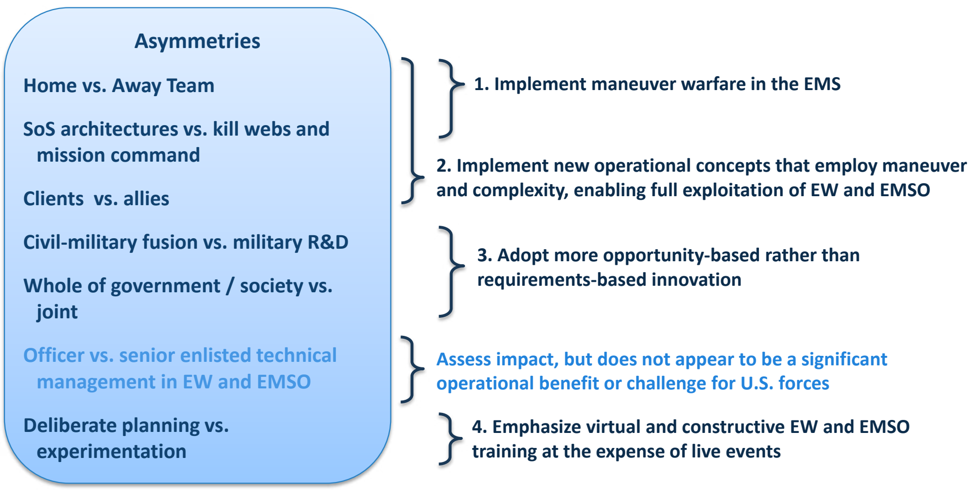
91 See footnote 1.

92 This approach was advocated in DSB, *21st Century Military Operations in a Complex Electromagnetic Environment*.

93 Hoehn, *U.S. Military Electronic Warfare Investment Funding*.

Instead of mounting a long-term effort with an uncertain likelihood of success, DoD should make bold moves now to gain an advantage in EW and EMSO by exploiting asymmetries in its competitions with China and Russia and taking affordable steps to mitigate its vulnerabilities. This chapter describes the initiatives DoD should undertake to pursue this approach, depicted in Figure 9.

FIGURE 9: ASYMMETRIES BETWEEN U.S., CHINESE, AND RUSSIAN EW AND EMSO CONCEPTS AND CAPABILITIES SHOULD BE ADDRESSED, MITIGATED, ACKNOWLEDGED, OR EXPLOITED BY DOD TO GAIN ENDURING EMS SUPERIORITY



Recommendations

1. Implement new operational concepts that employ maneuver and complexity, enabling full exploitation of EW and EMSO.

DoD should adopt new warfighting approaches that emphasize maneuver to take advantage of potential adversary force design and C2 vulnerabilities, as well as those that more fully exploit the capability of EW and EMSO to impact operational outcomes. Today's operational concepts rely on EW as an afterthought to improve survivability and EMSO to enable coordination and sensing. Instead, DoD's operational concepts should be designed such that they heighten the benefit gained from effective EW and EMSO.

As described in Chapter 2, PLA operational concepts and C2 processes are very different from those of the U.S. military. The PLA approaches to System Destruction Warfare, and systems warfare in general, establish SoSs at the outset of a confrontation that are designed to address likely scenarios and the opponent's expected forces and tactics. These include SoSs for EW and EMS operations. To be relatively responsive, most of these SoSs would need to be created and in place before a conflict. The PLA C2 process overseeing SoS operations depends on staff planning and consensus-based decisions, followed by decentralized execution. If plans need to change, staffs would re-plan operations and commanders would need to again reach consensus.

U.S. defense leaders have stated that the Chinese military is DoD's most pressing great power competitor. Therefore, DoD should emphasize operational concepts that counter the PLA's warfighting and C2 approaches. The PLA SoS architecture will be challenged to adjust operational relationships or the composition of EW and EMSO effects chains dynamically during an operation, particularly among forces in the field. Similarly, the PLA C2 process will have difficulty accommodating changes to plans and tactics once a mission is underway.

The U.S. military could undermine the confidence of PLA leaders in their force structure, operational concepts, and C2 by implementing new warfighting concepts that employ dynamic and complex force packages and tactics in the EMS and other domains to increase the adversary's uncertainty regarding a U.S. force's disposition and intentions. This approach is central to the concept of maneuver warfare, which seeks to prevent an enemy from reaching its objectives and allow friendly forces to achieve theirs by imposing multiple, simultaneous dilemmas on an opponent.[94]

Maneuver warfare in the EMS can amplify the impact of maneuver in other domains, creating greater adaptability for U.S. forces and complexity for an adversary. For example, an air strike that employs a small disaggregated group of manned and unmanned platforms and missiles may be able to circumvent air defenses using jamming, EMCON, and decoys to engage a target with munitions or high-power microwave (HPM) weapons without necessitating a costly rollback of adversary sensors and air defenses first.

Several emerging DoD operational concepts are pursuing variations on maneuver warfare that could degrade adversary responses and improve the force's ability to employ EW and EMSO. Although they still unproductively pursue a goal of attrition, the U.S. Army's MDO concept and the U.S. Navy's DMO concept both use more distributed formations to improve the survivability of forces, increase complexity for an adversary, better exploit EW, and enable more flexible employment of maneuver and fires.[95] The Navy also complements its DMO concept with Electromagnetic Maneuver Warfare (EMW), which marries maneuver in the maritime and air domains with maneuver in the EMS and space.[96] DARPA is also pursuing a new warfighting approach centered on maneuver called Mosaic Warfare, which relies on highly disaggregated forces, networked cognitive EMBM, and autonomous planning

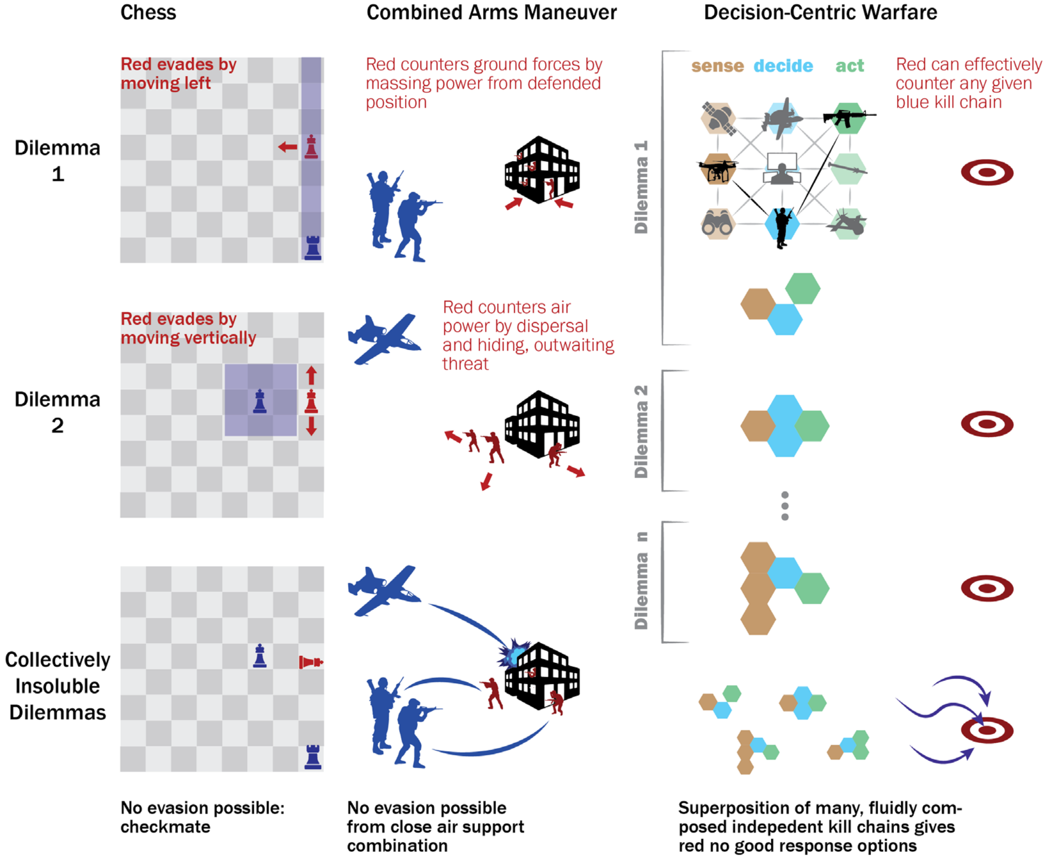
94 Maneuver warfare is contrasted with attrition warfare, which seeks to defeat an opponent by neutralizing or destroying enough of its forces to render it unable to achieve its objectives. (Robert Leonhard, *The Art of Maneuver: Maneuver Warfare Theory and AirLand Battle (*New York, NY: Ballantine Books, 1991, p. 21-23.)

95 TRADOC, *The Army in Multi-Domain Operations 2028*, pp. 32–44.

96 John Joyce, "Navy Expands Electromagnetic Maneuver Warfare for 'Victory at Sea'," *Navy News Service,* November 2, 2017.

and decision aids to improve U.S. force adaptability and impose greater complexity on adversaries.[97]

FIGURE 10: A MANEUVER APPROACH TO WARFARE WOULD ENABLE THE IMPOSITION OF MORE SIMULTANEOUS DILEMMAS ON AN ADVERSARY



Evolving force design and C2 for maneuver warfare

U.S. commanders would likely be hindered or precluded from effectively practicing maneuver warfare by the U.S. military's force design, which consists predominantly of large, self-contained multimission units. Because of their cost, U.S. forces will include too few of these individual units to enable sufficient distribution, adaptability, and recomposability to overwhelm the PLA's ability to adapt. Furthermore, large multimission units require protection, resulting in relatively predictable force packages, tactics, and dispositions.

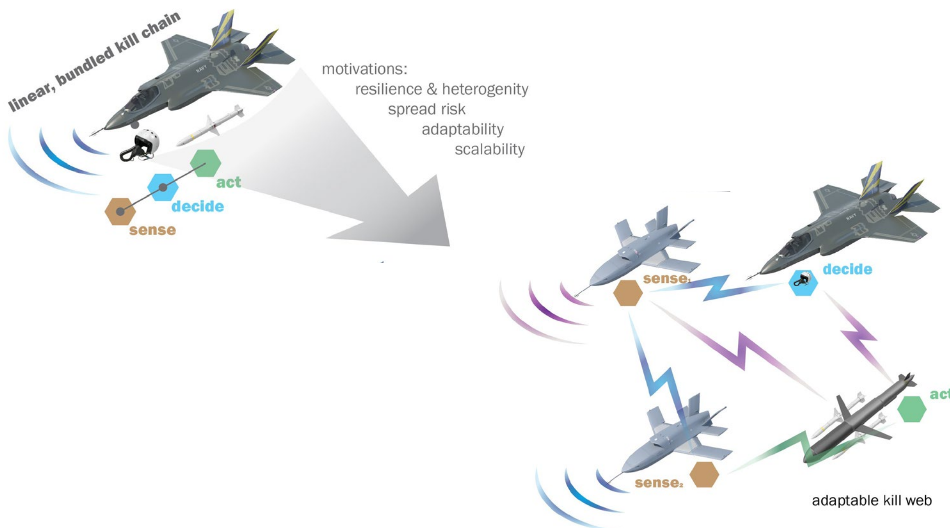
Even with a more disaggregated and recomposable force, today's C2 capabilities will limit the ability of the U.S. military to impose complexity and multiple dilemmas on adversaries. U.S.

97 "Strategic Technology Office Outlines Vision for 'Mosaic Warfare'," *news and events*, DARPA, August 4, 2017, available at https://www.darpa.mil/news-events/2017-08-04.

military leaders like to highlight the initiative and creativity of leaders employing “mission command” when delegated authority or when communications are lost with senior commanders.[98] However, the tools available to field commanders are insufficient to enable them to develop and plan creative operations. As a result, commanders, particularly junior ones who lack large planning staffs, will tend to fall back on doctrine, habits, and traditions that the enemy can predict. This shortfall will become more acute as U.S. forces pursue more distributed formations and communications become more contested.

DoD will need to evolve its force design and C2 processes to fully exploit the potential of maneuver warfare and the PLA’s potential lack of flexibility and responsiveness. These changes, however, do not need to be comprehensive. Replacing a small portion of today’s multimission ships, aircraft, or troop formations with smaller, cheaper and less multifunctional units would be enough to enable greater adaptability in U.S. forces packages while imposing considerable complexity on adversaries.

FIGURE 11: DISAGGREGATED RECOMPOSABLE UNITS VERSUS MONOLITHIC MULTIMISSION PLATFORMS AND FORMATIONS

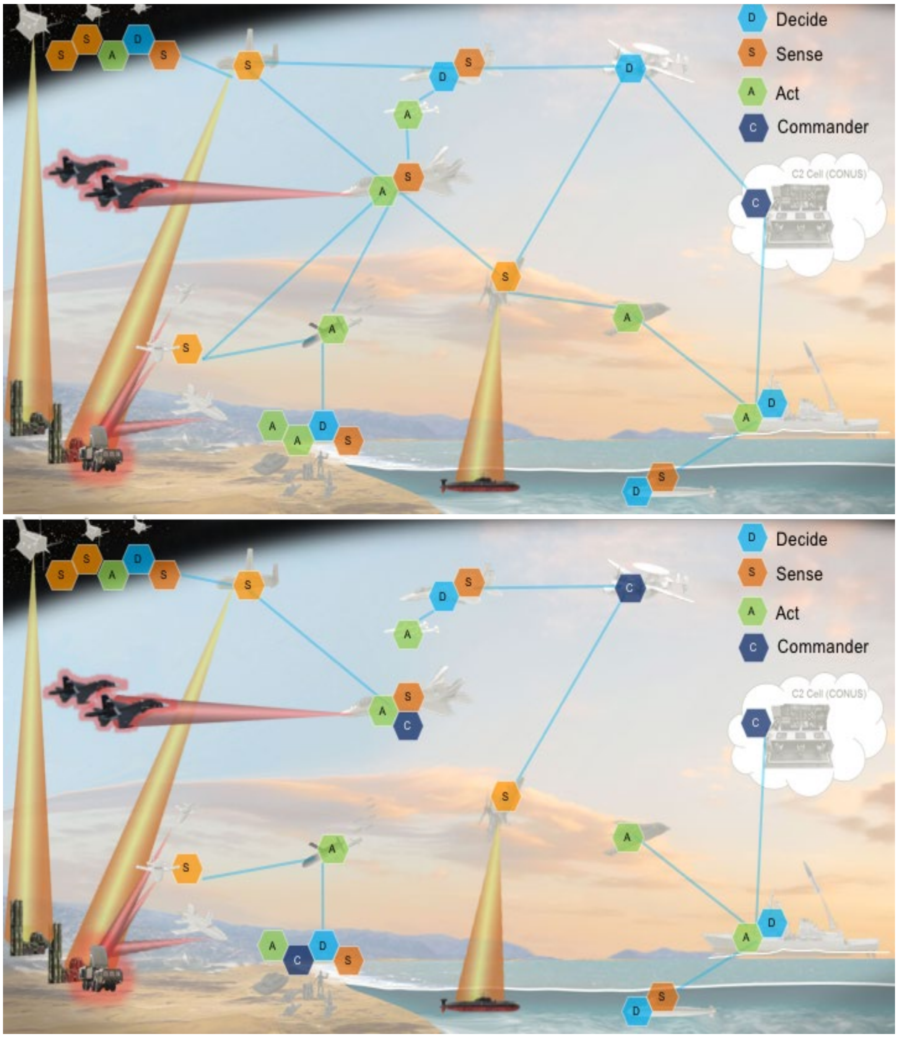


Instead of adopting completely new C2 processes, DoD should implement “context-centric C3” in which the C2 relationships of a force are based on communications availability, rather than attempting to build a communications architecture that will support a pre-determined C2 construct. In context-centric C3, a commander is in charge of those forces he or she is in communication with, subject to any trades made with other coordinating commanders. The essential element of this new C3 approach is the development of new planning tools that enable leaders up and down the chain of command to creatively plan, adapt, and recompose

98 Paul Hutchings, “The Philosophy of Mission Command and the NCO Corps,” *NCO Journal,* February 21, 2018.

their forces and operations. Planning tools like those needed have been demonstrated and are being developed by multiple DoD efforts, such as the DARPA Adapting Cross-Domain Kill Chains (ACK) and Complex Adaptive System Composition And Design Environment (CASCADE) programs.[99]

FIGURE 12: CONTEXT-CENTRIC C3 COULD REDUCE IMPACT OF COMMUNICATION DISRUPTIONS



Instead of building communications to meet a desired C2 structure, C3 architectures should align forces to commanders based on the available communications. In the top figure, a centralized commander is able to manage and communicate with a large, widely dispersed force. In the bottom figure, communications are degraded, and subordinate leaders must take mission command and pursue tasks aligned with the forces they can communicate with, with their planning facilitated by the machine-enabled control system.

99 Dan Javorsek, “Adapting Cross-Domain Kill Chains (ACK),” *program information*, DARPA, available at https://www.darpa.mil/program/adapting-cross-domain-kill-webs; and John S. Paschkewitz, “Complex Adaptive System Composition And Design Environment (CASCADE),” *program information*, DARPA, available at https://www.darpa.mil/program/complex-adaptive-system-composition-and-design-environment.

Exploiting EW and EMSO concepts and capabilities

EW and EMSO will be key elements of future maneuver warfare concepts. A more disaggregated and recomposable force will be inherently more difficult for an adversary to assess; smaller, less multifunctional units will be easier to obscure using jamming or emulate using decoys. As a result, EW operations are likely to be more effective with a maneuver force than one designed to fight an attrition battle.

Compared to traditional multimission platforms and formations, a force that includes more unmanned vehicles would be better able to reduce and manage its emissions as part of EMSO. Distributed unmanned vehicles could be employed for passive sensing techniques that benefit from multiple sensors such as passive coherent location (or passive radar), multistatic radar, and IR search and track. This would enable geolocation or could provide multiple aspects for wave front analysis. Less multifunctional units could also require fewer communications than multimission platforms and formations because of their limited functionality and a reliance by commanders on context-centric C3.

2. Adopt more opportunity-based rather than requirements-based innovation

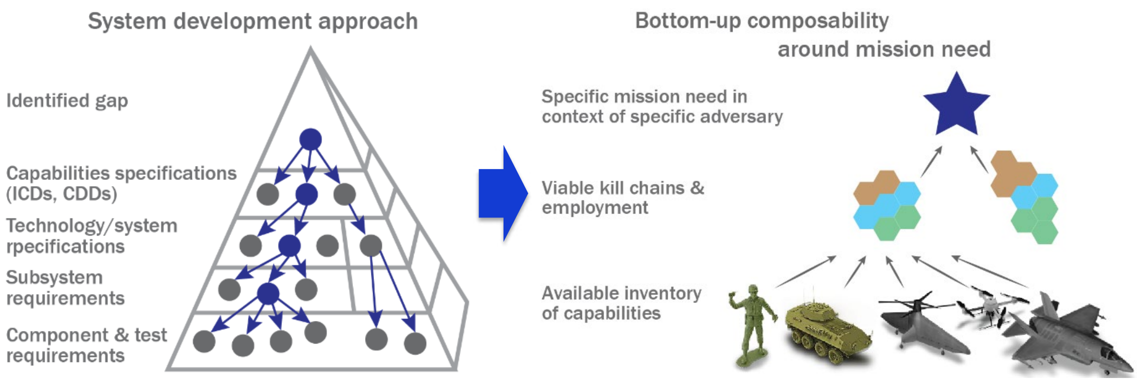
DoD should pursue approaches to capability development that would improve its ability to incorporate commercial technologies and accelerate the transition of new EW and EMS technologies into fielded systems. This would help mitigate the ability of Chinese and Russian militaries to integrate commercial and government R&D efforts. It would also enable U.S. forces to exploit the potential for cognitive, adaptive, networked, and multifunction EW and EMSO systems to undermine the static SoS or legacy EW and EMSO technologies of the PLA and Russian Armed Forces, respectively.

Moving toward a force that is more disaggregated and recomposable has significant implications for how DoD identifies and develops new capabilities. Today's systems development approach identifies requirements for new programs by analyzing the ability of the future force to execute planned operational concepts against projected threats. This approach tends to focus on gaps where U.S forces will fall short against threats, resulting in needs for new capabilities. In addition to relinquishing the initiative in capability development to the adversary, requirements-driven systems development incorporates numerous assumptions regarding potential future operational scenarios and threat capabilities and tactics. It also links future requirements to current or planned U.S. operational concepts and tactics, potentially constraining future innovation by limiting the capability of new systems. As a result, systems emerging from a requirements-driven development process may be obsolete.

The gap-driven requirements process is useful for foundational capabilities that will operate in more predictable ways, including acting as the deployment and C2 platform for more disaggregated forces. These foundational units, such as aircraft carriers, strategic bombers, and nuclear submarines, also provide the endurance and predictability needed for peacetime missions and for situations where assurance of allies and deterrence of some adversaries depends on a visible and understood posture.

As DoD incorporates more disaggregated units like unmanned vehicles, fire teams or platoons, and small combatant ships into the force, the traditional requirements-driven systems development approach will become less relevant. Disaggregated units are intended to be versatile and act as elements of a composable force. Therefore, their value will derive from the performance of a force package in applicable missions when the unit is introduced.

FIGURE 13: DOD WILL NEED TO ADOPT ALTERNATIVE INNOVATION PROCESSES THAT AUGMENT TODAY'S GAP-DRIVEN SYSTEMS DEVELOPMENT APPROACH



Whereas a requirements-driven development process identifies needs for new capabilities, a systems development process for composable units would identify opportunities to improve the force's performance in important missions. A composable force will not have gaps to fill, per se, because the force will compose itself to accomplish its tasking, although the delay and losses incurred may be unsatisfactory.

The opportunity-based systems development process would assess new ideas through a series of challenges regarding their operational value, technical feasibility, interoperability, sustainability, and other metrics. Whereas today program managers are charged with developing a new system to deliver a product at the end, in opportunity-based systems development program managers would focus on culling out bad ideas by showing how they don't add operational value or are infeasible or impractical. In addition to enabling DoD to consider a wider range of new capability and concept ideas, this approach would also reduce the likelihood a bad idea consumes significant funding before it is cancelled.[100]

Opportunity-based capability development is not a significant departure from many current DoD capability development efforts. The Services' rapid capability development offices pursue a form of opportunity-based capability discovery, and DARPA has a high percentage of programs that are exploring potential opportunities, rather than filling current or anticipated

100 This approach is described in more detail in John D. Evans and Ray O. Johnson, "Tools for Managing Early-Stage Business Model Innovation," *Research-Technology Management*, September–October 2013, p. 52.

capability gaps. These efforts should be expanded by the Services to support the development of mission systems across a wider swath of programs, although manned platform development may continue to be based on requirements.

3. Implement maneuver warfare in the EMS

The U.S. military has an inherent EW and EMSO disadvantage as an expeditionary force. Because they are mobile and lack the space for large, high-gain passive receivers, U.S. platforms and troop formations use active radars and jammers to achieve the range, accuracy, and responsiveness needed for air defense or to quickly find and target enemy forces. Active emissions, however, make U.S. forces easier to detect with wide-area electronics intelligence and ES sensors, which adversaries on the strategic defense like China and Russia can establish on their own territory. The expeditionary nature of U.S. forces also enables the PLA and Russian Armed Forces to predict likely avenues of approach, so they can emplace long-range HF sensors where they will provide the most operational benefit.

Shift to predominantly passive and multistatic sensing

To mitigate this vulnerability, in contested areas the U.S. military should use passive or multistatic sensing almost exclusively, complemented by LPI/LPD communications and electronic countermeasures. Some missions, however, will need to continue relying on active sensors and countermeasures, such as air and missile defense. To balance these considerations and provide a framework to assess when and where active, passive, or multistatic EW and EMSO capabilities should be employed, the U.S. military should pursue a goal of achieving EMS superiority rather than solving individual capability gaps (such as the ability of a specific standoff jammer to obscure or deceive a specific air defense radar). In this context, EMS superiority is taken to mean the ability to operate in the EMS while denying it to adversaries across an intended area and for a determined duration.

Treat the EMS as an operational domain

Gaining superiority instead of defeating individual systems is how land, air, and naval warfare is assessed and conducted. Although specific systems or platforms likely to encounter each other are often compared, capability needs are generally assessed in the context of an operational situation in which the goal is overall superiority, rather than system vs. system success. In naval warfare, the ability of a surface combatant to find and successfully destroy a threat submarine is not considered a high priority because anti-submarine warfare (ASW) will often employ offboard unmanned sonar arrays and aircraft-launched torpedoes. In land operations, tanks of opposing forces are often compared, but the ability of a tank to defeat another tank is less important in a force that also has attack aircraft and anti-tank platoons.

To pursue the ability to gain EMS superiority, DoD should treat the EMS as an operational domain like the air, land, sea, space, and cyberspace. Even if not formally enacted into doctrine, adopting a domain construct for the EMS will enable analyses of EW and EMSO missions to reveal opportunities for different tactics or alternative capabilities to obviate or defeat threats that would otherwise create the need for a new system under DoD's current requirements-driven systems development approach. For example, a combination of emissions controls (EMCON), expendable stand-in jammers, and standoff weapons could prevent a new adversary air defense radar from targeting U.S. attack aircraft, eliminating the need to improve or build a new standoff jammer to do so.

Treating the EMS as an operational domain is also more appropriate than establishing broader constructs like an information domain. Thinking of the EMS as a domain facilitates concept and capability analysis or decision-making because it is a place governed by well-established physical laws in which military forces are operating. In contrast, information is content moving through the EMS or cyberspace domain that has subjective effects depending on the source, recipient, and context.

Implement maneuver warfare in the EMS

A domain construct will support the implementation of maneuver warfare in the EMS rather than attrition warfare. Today's approach to EMS operations reflects an attrition warfare mindset, in which actions such as EA, ES, EP, communications, and sensing are treated as distinct operations; the goal is for systems performing these functions to overcome the opposing system. In a domain construct, these actions would be considered as interrelated operations that can be employed in concert to accomplish the commander's intent and tasking through maneuver in the EMS.

Maneuver warfare encompasses two main mechanisms for defeating an opponent: *dislocation*, in which the opponent is prevented from achieving its objectives or achieving them on its desired timeline; and *disruption*, in which the maneuver force directly degrades and undermines the cohesion of the adversary force.[101] In the EMS, dislocation could be pursued by adopting more passive and multistatic sensors that prevent an opponent from rapidly targeting and identifying U.S. or allied forces, coupled with self-protection EA and directed energy weapons to improve the air defense capacity of friendly forces.

EW and EMSO could enable disruption by using offboard stand-in jammers and decoys to improve the survivability of forces conducting physical attacks, or by using directed energy weapons like HPM carried by UAVs and standoff missiles to damage enemy electrical and electronic equipment.

101 Robert Leonhard, *The Art of Maneuver: Maneuver Warfare Theory and AirLand Battle* (New York, NY: Ballantine Books, 1991), pp. 66–74.

FIGURE 14: PASSIVE AND MULTISTATIC SENSING SHOULD BE USED IN CONCERT WITH EW AND DIRECTED ENERGY AIR AND MISSILE DEFENSE TO DISLOCATE ADVERSARY OFFENSIVE OPERATIONS

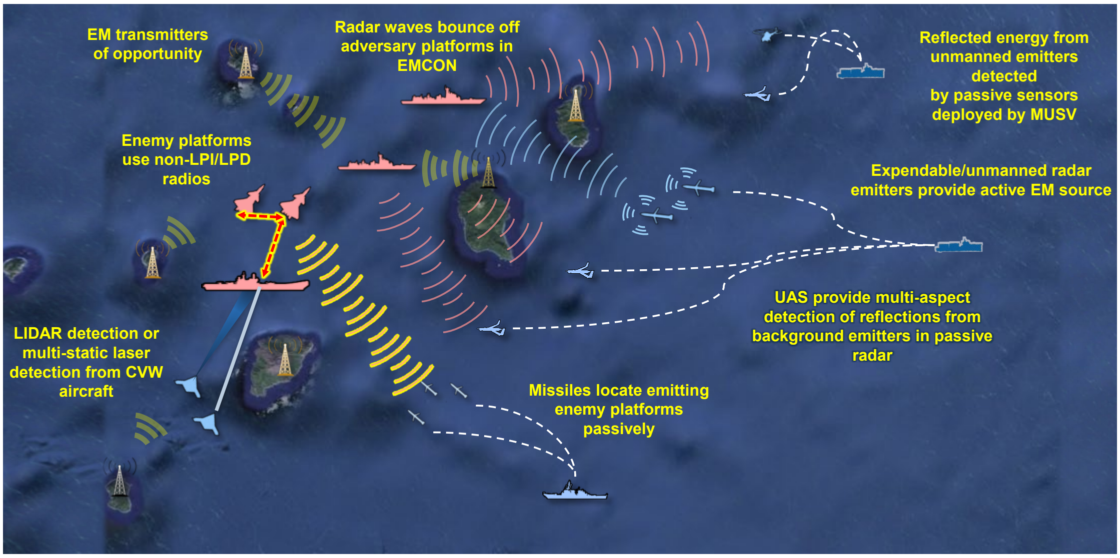
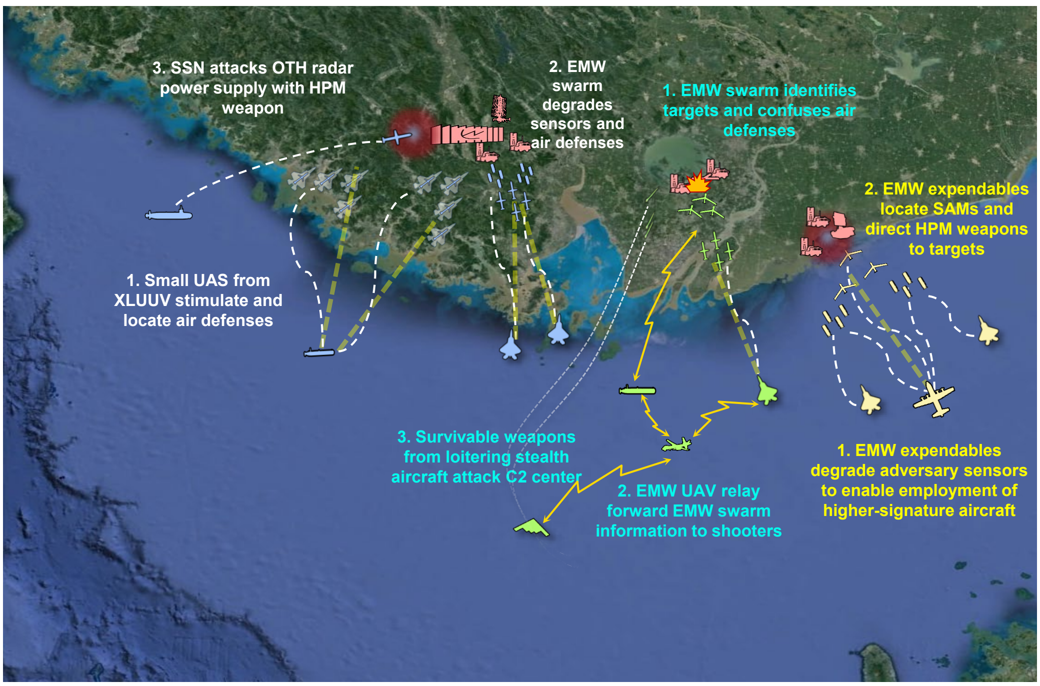


FIGURE 15: EXPENDABLE JAMMERS AND DECOYS, COMPLEMENTED BY DIRECTED ENERGY WEAPONS, SHOULD BE USED TO DISRUPT ADVERSARY FORCES



Field more networked EW and EMSO systems and EMBM capabilities

Conducting maneuver warfare in the EMS will prioritize the fielding of several new technologies that were highlighted in the DoD EW Strategy but are slowly making their way into operational systems today. Most important among them is networked EW and EMSO systems. Networking can enable a set of passive RF or IR receivers to achieve the gain and precision to map the surrounding environment and target enemy forces. Multistatic radar and light direction and ranging (LIDAR) also rely on communications between illuminators, which could be expendable unmanned vehicles or emitters of convenience, like mobile phone towers, and passive receivers on manned or unmanned platforms. Networking can also allow traditional monostatic radar to achieve LPI/LPD characteristics by enabling passive sensors to obtain a bearing or approximate range to a potential target, allowing a radar to reduce its beamwidth and power to the minimum needed for detection or tracking.

Networking will also be essential to future EA operations. Today, EA actions consist predominantly of self-protection jamming by a platform or escort jamming, in which an EA platform protects another platform. Both types of jamming create counterdetection risks. Future EA operations should employ relatively expendable offboard jammers and decoys, which may be launched by the protected platform or operate independently. Networking would help ensure the EA actions of the offboard system are coordinated with the protected platform's maneuvers and assessment of the threat's characteristics and intentions.

With the expected proliferation of EMS systems in U.S. and allied forces, networking will be needed to coordinate and deconflict EW and EMSO actions. A lack of coordination could result in problems such as an LPI/LPD radar inadvertently illuminating friendly forces, EA operations degrading passive sensors or illuminating friendly units, or communications signals being intercepted by enemy receivers. Some EMBM software programs under development by DoD could enable this coordination; if they are resident on each EW and EMSO system, EMBM systems could reduce the communications needed to coordinate EMS operations.

Adopting EMBM and networked EW and EMSO could make the force more vulnerable to communications jamming and exploitation. Context-centric C3, as described previously, would mitigate this vulnerability by constraining the network to those participants that are in communication with the commander. To improve the ability of networked EW and EMSO systems to remain effective as the network collapses due to communications jamming, each system should have multiple functions.

Proliferate ES capabilities and field more multifunction EW and EMSO systems

Every EW and EMSO system should incorporate ES functionality to help achieve LPI/LPD characteristics, improve the effectiveness of EW actions, and coordinate EW or EMSO actions with minimal communications. Passing sensor data to communication systems can help them avoid threats by moving away from jamming in frequency or time, changing the direction of transmissions to reach friendly units and avoid potential enemy receivers, and adjust power levels to be just sufficient to reach the intended recipients. Similar benefits would accrue to radars, jammers, and decoys, which all need to know the location of threats to avoid or where to focus emissions in time, space, and frequency to engage targets. Having an organic ES capability would also enable each system to sense the environment and coordinate friendly force actions in the EMS using onboard EMBM programs without communicating to other network participants.

The expense and complexity of incorporating ES functionality would not be significant, as most modern antenna arrays are capable of transmitting and receiving, and the software and processing to conduct ES operations would not significantly complicate system designs. The U.S. Army is making some progress in this direction by integrating its EW and signals intelligence (SIGINT) units.[102]

Similar to the benefit of incorporating ES functionality into each EW and EMSO system, making more new EW and EMSO systems multifunctional would increase the variety of locations from which sensing or effects could be provided, as well as help an EW or EMSO network remain effective even if the network loses participants due to enemy communications jamming. Having more EW and EMSO systems capable of sensing, communicating, jamming, or decoying would also provide greater adaptability to U.S. forces and increase the complexity imposed on adversaries, consistent with the maneuver warfare concepts described above.

Field cognitive EMS capabilities

Although an automated system could employ multiple EW and EMSO functions to achieve an operator's desired effects, fully exploiting the ability of networked, multifunction EW and EMSO systems to operate at machine speed will require operators to yield some decision-making to the EW or EMSO system. DoD will need to field more adaptive and cognitive algorithms in existing and planned EW and EMSO systems to take advantage of the capabilities made possible by improving hardware and networking. Today, adaptive algorithms that can react to adversary actions are reaching EW systems in operating forces.[103] These programs should be accelerated, along with efforts to establish testing processes and data governance procedures for future cognitive EW and EMSO systems.

Solve interoperability challenges in standards and security

The most significant impediments to networked EW and EMSO and EMBM are creating interoperable data transmission standards and the varied security levels at which different EW and EMSO systems operate. DoD is advancing several programs that could act as gateways between communication standards, such as the Battlefield Airborne Communications Network (BACN) node, or translate between them, such as DARPA's System of Systems Integration Test and Experimentation (SoSITE) program, which developed the System

102 Mark Pomerleau, "The Army Wants to Build a Better Signals Intelligence Force," *C4ISRNet,* July 19, 2018.

103 DoD, "Integrated Defensive Electronic Countermeasures (IDECM)."

of Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) technology for ad-hoc interoperability.[104]

Capabilities are also being developed to enable information to be passed automatically between systems operating at different security levels. Although less mature than communications interoperability solutions, multilevel security systems using a combination of autonomous routing protocols and AI-enabled language processing hold the promise of enabling a network of EW and EMSO systems to seamlessly share data, while protecting the security associated with the most sensitive sensing data or transmissions.[105]

4. Emphasize virtual and constructive EW and EMSO training at the expense of live events

The U.S. military lacks the training and experimentation opportunities of the Russian Armed Forces in Syria and Ukraine or the PLA's instrumented ranges. DoD will need to restore its EW and EMSO range facilities for U.S. forces to regain their operational proficiency, develop new operational concepts and tactics, and evaluate the impact of new capability opportunities.

DoD is following a range improvement plan designed to modernize its threats, network adversary radar and EW systems, provide improved instrumentation, and enable more responsive threat capabilities. DoD progress on this plan has been slow, and, while affordable in the overall defense budget, the cost to upgrade range facilities is significant. In light of the lack of progress, Congress directed DoD to provide a new strategic plan for training and test ranges in the FY 2019 NDAA.[106]

However, attempting to upgrade live open air ranges to modern threats is an ineffective approach to improve operator proficiency and develop new tactics and operational concepts. Even if the investment is made to establish agile, networked, and modern sensor and EW threats at DoD ranges, operational security concerns will likely preclude fully exploiting the improved facilities. The Chinese and Russian governments deploy robust electronic intelligence (ELINT) and SIGINT satellite constellations that would likely monitor DoD range activity. As a result, U.S. forces would be reticent to employ or practice their most effective

104 "Battlefield Airborne Communications Node (BACN)," Northrop Grumman, available at https://www.northropgrumman.com/Capabilities/BACN/Pages/default.aspx; and Jimmy Jones, "System of Systems Integration Technology and Experimentation (SoSITE)," *program information*, DARPA, available at https://www.darpa.mil/program/system-of-systems-integration-technology-and-experimentation.

105 "Secure Handhelds on Assured Resilient Networks at the Tactical Edge (SHARE)," DARPA, available at https://www.darpa.mil/work-with-us/secure-handhelds-on-assured-resilient-networks-at-the-tactical-edge.

106 OSD, "Department of Defense's Comprehensive Training Range Sustainment Plan," in *2012 Sustainable Ranges Report*, Annual Report to Congress (Washington, DC: DoD, April 2012), available at https://www.denix.osd.mil/sri/policy/reports/report-to-congress-on-sustainable-ranges/chapter-4-department-of-defense-s-comprehensive-training-range-sustainment-plan/; DoD Inspector General, Audit of Training Ranges Supporting Aviation Units in the Indo-Pacific Command (Washington, DC: DoD, April 17, 2019), available at https://media.defense.gov/2019/May/08/2002129129/-1/-1/1/DODIG-2019-081.PDF; and U.S. Congress, John McCain National Defense Authorization Act for 2019, Section 2862, August 23, 2018, available at https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

techniques. Moreover, incorporating the most advanced threats at training ranges would potentially reveal to competitors the extent and nature of U.S. intelligence-gathering.

Instead of upgrading its training ranges at great cost to gain a modest operational benefit, DoD should shift its emphasis for EW and EMSO practical training to virtual and constructive facilities. Virtual training systems using simulators with human operators would enable EW and EMSO concept development, tactics innovation, and proficiency training against the most challenging threats at all security levels.

Live EW and EMSO training would still be needed to ensure safe and proficient system operations in the field. These operations, however, could focus on less-modern threats or could employ closed-loop radar, communication, and EW systems. Closed-loop systems could use a secure datalink to communicate the intended signal characteristics and operations of each system to enable open-air training, but without using the actual emissions each system would produce. Closed-loop and legacy EW and EMSO systems would be an affordable way to modestly upgrade live ranges that allows more funding to go to virtual and constructive training capabilities.

Conclusion

DoD cannot continue on its current path of attempting to gain EMS superiority by incrementally improving individual systems to avoid or target new threats as they emerge. Today's requirements-based approach to EW and EMSO systems development is too unfocused, will take too long to reach fruition, is potentially unaffordable, and cedes the initiative to America's great power competitors.

Instead of reacting to adversary moves with its own countermoves, DoD should move in a new direction to gain the ability to achieve EMS superiority and take back the initiative in EW and EMSO. This approach would focus EW and EMSO capability development on implementing concepts for maneuver warfare that seek to create adaptability for U.S. forces and complexity for adversaries. The implications of this shift would include opening new pathways for R&D and innovation, treating the EMS as an operational domain, rebalancing priorities for EW and EMSO technologies, and shifting training to virtual and constructive systems.

If the DoD does not mount a new more strategic and proactive approach to fighting in the EMS and developing the requisite capabilities, adversaries could be emboldened to continue their ongoing efforts to gain territory and influence on their peripheries at the expense of U.S. allies and partners. Demonstrating the ability to survive and fight in a contested EMS could help U.S. forces slow Chinese and Russian sub-conventional or gray-zone operations and deter or dissuade these competitors from more aggressive approaches to their objectives.

LIST OF ACRONYMS

AEA	airborne electronic attack
BACN	Battlefield Airborne Communications Network
C2	command and control
CFT	Cross-Functional Team
CMC	Central Military Commission
CNAD	Conference of National Armaments Directors
CTC	combat training center
DARPA	Defense Advanced Research Projects Agency
DMO	Distributed Maritime Operations
DSB	Defense Science Board
ELINT	electronic intelligence
EMCON	emissions control
EMW	Electromagnetic Maneuver Warfare
EWPMT	EW Planning and Management Tool
GPS	Global Positioning System
HF	high frequency
HPM	high-power microwave
IDECM	Integrated Defensive Electronic Countermeasures
JCIDS	Joint Capabilities Integration and Development System
JSDF	Japan Self Defense Force
LIDAR	light direction and ranging
LPI/LPD	low-probability of intercept/low probability of detection
MDA	Missile Defense Agency
MDO	Multi-Domain Operations
NATO	North Atlantic Treaty Organization
NEWAC	Electronic Warfare Advisory Committee
OSD	Office of the Secretary of Defense
PGM	precision-guided munition
PLAN	PLA Navy
RF	radio frequency
RTSO	Real-Time Spectrum Operations
SAR	Selected Acquisition Report
SIGINT	signals intelligence
SoSITE	System of Systems Integration Test and Experimentation
STITCHES	System of Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems
TRADOC	U.S. Army Training and Doctrine Command
UAV	Unmanned Aerial Vehicle
SHAPE	Supreme Headquarters Allied Powers Europe
USIA	United States Information Agency

CSBA

Center for Strategic and Budgetary Assessments

1667 K Street, NW, Suite 900
Washington, DC 20006
Tel. 202.331.7990 • Fax 202.331.8019
www.csbaonline.org