United States Government Accountability Office

Report to Congressional Committees

August 2019

FUTURE WARFARE

Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations

GAO-19-570

GAO Highlights

Highlights of GAO-19-570, a report to congressional committees

August 2019

FUTURE WARFARE

Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations

Why GAO Did This Study

The rise of great-power competitors, such as China and Russia, prompted the Army to transform the way it plans to fight. The Army is developing a new warfighting concept to guide how its forces will engage jointly with other services in multiple domains, especially in cyber and space.

The House Armed Services Committee included a provision in House Report 115-200 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 for GAO to review the Army's implementation of the concept. Among its objectives, this report addresses (1) how the Army is changing its doctrine, organizations, and training in order to execute multi-domain operations; and (2) the extent to which the Army has established new cyber and electronic warfare units, including any challenges faced by these units, and whether the Army assessed risks associated with its plan to establish these units.

GAO reviewed Army concepts, doctrine, force design, and training documents concerning multi-domain operations. GAO also interviewed Army and Department of Defense officials.

What GAO Recommends

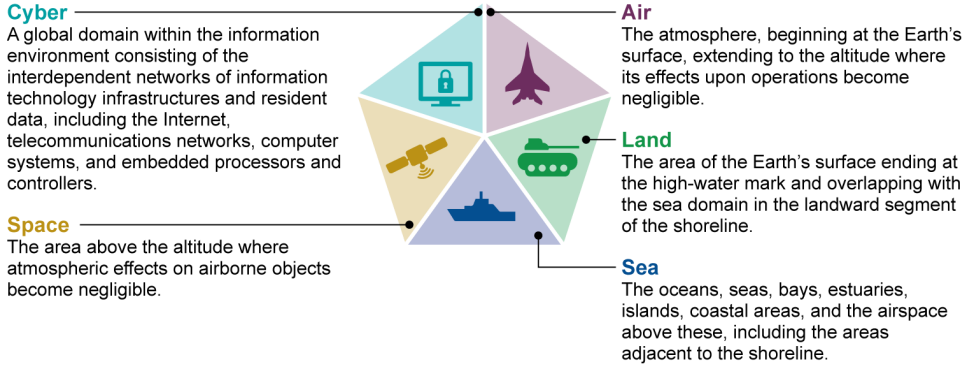
GAO is making three recommendations, including that the Army comprehensively assess the risk of staffing, equipping, and training the cyber and electronic warfare units that it has activated at an accelerated pace, and to do so for new organizations it plans to activate in an accelerated manner for multi-domain operations. The Army concurred with one recommendation and partially concurred with two recommendations. GAO clarified the recommendations, as discussed in the report.

View GAO-19-570.For more information, contact John Pendleton at (202) 512-3489 or pendletonj@gao.gov.

What GAO Found

The Army is changing aspects of its doctrine, organizations, and training to develop a force that can effectively engage great-power competitors—Russia and China—through multi-domain operations by 2028. Multi-domain operations present adversaries with multiple challenges across multiple domains (land, air, sea, cyber, and space) in contested environments. To this end, the Army is revising its doctrine to guide how the force and specific units will function. The Army is also reorganizing its force by creating new units to conduct missions in multiple domains and by updating the responsibilities of key Army formations, such as Army divisions. Also, the Army is training its combat forces for multi-domain operations in part by increasing the focus on cyber operations.

The Five Warfighting Domains Envisioned by the Army Operating Concept



Source: GAO analysis of Department of Defense information. | GAO-19-570

The Army is establishing new cyber and electronic warfare units for multi-domain operations, but did not fully assess the risk of activating some units at an accelerated pace and is experiencing staffing, equipping, and training challenges. For example, the Army activated a cyber battalion in December 2018, and as of March 2019, this unit was understaffed by more than 80 percent. Army guidance directs the Army staff to conduct assessments on new units to determine whether the Army can staff, equip, and train these organizations. However, Army leadership believed the threats justify developing these units at an accelerated pace. Consequently, the Army did not assess the staffing, equipping, and training risk before activating one unit, and only conducted an initial risk assessment before activating a second unit. As a result, senior Army leaders may not know what other challenges could arise, such as sustainment, as the units grow in capability. Army officials told GAO that as these units evolve, it is uncertain when more comprehensive risk assessments would take place. The Army has previously accelerated the activations of other units when it saw fit to do so, and is considering creating other new units for multi-domain operations. If the Army does not assess risks for units activated at an accelerated pace, those units may be unable to effectively conduct multi-domain operations.

Contents

Letter		1
	Background	5
	The Army Is Changing Its Doctrine, Organizations, and Training to Execute Multi-Domain Operations	10
	The Army Is Establishing New Cyber and Electronic Warfare Units, but Units Are Facing Staff, Equipment, and Training Shortfalls in Part Due to Incomplete Risk Assessments	15
	The Army Engaged with the Joint Staff and Other Services and Envisions Opportunities for Further Coordination	22
	Conclusions	24
	Recommendations for Executive Action	25
	Agency Comments and Our Evaluation	25
Appendix I	Comments from the Department of the Army	29
Appendix II	GAO Contact and Staff Acknowledgments	32
Table		
	Table 1: The Army Is Activating New Units at an Accelerated Pace Resulting in Staff Shortages as of March 2019	16
Figures		
	Figure 1: The Five Warfighting Domains Envisioned by the Army Operating Concept	6
	Figure 2: The Army's Expanded Battlefield in Multi-Domain Operations	9
	Figure 3: Concepts Shape Army Doctrine, Organizations, and Training	10

Abbreviations

ARSTRUC	Army Structure Memorandum
CTG	Command Training Guidance
DOD	Department of Defense
FORSCOM	Army Forces Command
GAO	Government Accountability Office
ICEWS	Intelligence, Cyber, Electronic Warfare, and Space
TRADOC	Army Training and Doctrine Command

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

August 15, 2019

Congressional Committees

In recent years, the Department of Defense (DOD) and the Army have cited growing concerns about the ability to operate in contested security environments. After a decade of counterinsurgency operations in Iraq and Afghanistan, and what the unclassified *Summary of the 2018 National Defense Strategy* called strategic atrophy, DOD concluded that its competitive military advantage is eroding.[1] Several DOD reports, testimonies, and guidance all refer to the threats posed by both great-power competitors—particularly China and Russia—and other adversaries, now and into the future.[2] These threats are defined by rapid technological change, competition with the United States through operations below the threshold of armed conflict, and potential challenges from adversaries in every operating domain, especially cyber and space.[3]

Against this backdrop, the Army has been developing a new Army Operating Concept, which the Army is using to define how its forces will engage jointly with the other services for the task of deterring and defeating Chinese and Russian aggression in both competition and conflict. The Army calls this concept *The U.S. Army in Multi-Domain Operations 2028*, and it would enable the Army to confront adversaries in contested environments by presenting those adversaries with multiple

[1]DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Jan. 19, 2018).

[2]See Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, D.C.: 2017); Mark T. Esper, Secretary of the Army, and General Mark A. Milley, Chief of Staff of the Army, *The Posture of the United States Army,* testimony before the Senate Armed Services Committee, 115th Cong., 2nd sess., April 12, 2018; Department of Defense, *Quadrennial Defense Review* (Washington, D.C.: March 4, 2014). Great-power competitors are countries with diplomatic, informational, military, and economic capacity that are nearly comparable to that of the United States, and that are capable of waging large-scale conventional war.

[3]A domain is an area of activity within the operating environment in which operations are organized and conducted. For example, the Army recognizes five domains: land, air, sea, cyber, and space.

challenges across multiple domains (land, air, sea, cyber, and space).[4] The multi-domain operations concept will significantly affect Army doctrine, organizations, and training in the coming years.[5]

The Army's effort to rethink its overarching warfighting concept comes at a time when it is also undertaking a significant effort to modernize the force, while also rebuilding and sustaining the readiness of the current force.[6] In September 2018, we reported that the Army had reprioritized tens of billions of dollars in planned modernization spending for new priorities that support multi-domain operations, and also had established a new Army Futures Command to provide additional guidance for its modernization effort. In that report, we found that the Army had set decisively defeating great-power competitors as an overarching objective, but had not established processes for evaluating its modernization efforts against this objective, and had not completed a cost analysis of its near-term modernization efforts.[7] Further, we also reported in January 2019 that establishing the Army Futures Command creates unique opportunities for the Army to improve its modernization efforts and that the Army has generally applied leading management practices, such as well-defined team goals and senior management support, to its modernization. However, we also reported that the Army may be beginning weapon systems development before technology is sufficiently mature. This raises the risk that the resulting systems could experience

[4]Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Dec. 6, 2018). Throughout this report we may also refer to the Army's multi-domain operations concept as the "Army Operating Concept" or "the Army's concept" depending on the context. These terms all refer to the Army's multi-domain operations concept.

[5]The Army defines "doctrine" as fundamental principles, with supporting tactics, techniques, procedures, and terms and symbols, used for the conduct of operations and which the operating force, and elements of the institutional Army that directly support operations, guide their actions in support of national objectives. It is authoritative but requires judgment in application. See Army Doctrine Publication No. 1-01, *Doctrine Primer* (Sept. 2, 2014).

[6]GAO, *Army Readiness: Progress and Challenges in Rebuilding Personnel, Equipping, and Training*, GAO-19-367T (Washington, D.C.: Feb. 6, 2019).

[7]GAO, *Army Modernization: Actions Needed to Measure Progress and to Fully Identify Near-Term Costs,* GAO-18-604SU (Washington, D.C., Sept. 28, 2018). In this report, we recommended that the Army develop a plan to finalize processes for evaluating how its near-term investments contribute to its ability to decisively defeat a great-power competitor, and also that the Army finalize its cost analysis of near-term investments, and report these estimates to Congress. DOD concurred with both recommendations, and as of May 2019 the Army had taken steps to implement both of them.

cost increases, delivery delays, or failure to deliver desired capabilities.[8] We also testified on these issues in May 2019.[9]

Recognizing the significance of this effort and the need for multi-service involvement, the House Armed Services Committee included a provision in House Report 115-200 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 for us to review the Army's progress in implementing the new warfighting concept.[10] This report addresses (1) how the Army is changing its doctrine, organizations, and training in order to execute multi-domain operations; (2) the extent to which the Army has established new cyber and electronic warfare units, including any challenges faced by these units, and whether the Army assessed risks associated with its plan to establish these units; and (3) how the Army has engaged with the Joint Staff and other services to develop its new warfighting concept.

To address our first objective, we reviewed the Army's concepts related to multi-domain operations. We reviewed Army doctrine—the fundamental principles by which the Army guides actions in support of its objectives—related to overall operations, cyber operations, and fires, which includes artillery, rockets, and missiles. We reviewed force structure documents, such as force design updates, Army Structure Memorandums, and other associated briefings related to planned changes, as well as changes being considered for the future.[11] We reviewed strategies related to different types of training, in particular those dealing with cyber operations training and electronic warfare. We spoke with officials at Army headquarters, Army Futures Command, and Army Training and Doctrine Command (TRADOC). At Army headquarters, we met with

[8]GAO, *Army Modernization: Steps Needed to Ensure Army Futures Command Fully Applies Leading Practices*, GAO-19-132 (Washington, D.C.: Jan. 23, 2019). We made four recommendations in this report, including that the Army follow leading management practices for maturing technologies to a higher level, and also capture lessons learned from its modernization cross-functional teams. DOD concurred with all four recommendations. As of May 2019 the Army had not implemented the recommendations.

[9]GAO, *Army Modernization: Army Should Take Steps to Reduce Risk,* GAO-19-502T (Washington, D.C.: May 1, 2019).

[10]See H.R. Rep. No. 115-200, at 108-109 (2017).

[11]Army, *Army Structure (ARSTRUC) Memorandum 2020-2024* (Dec. 8, 2017). Army, *Addendum 1 to Army Structure (ARSTRUC) Memorandum 2020-2024* (June 6, 2018). Army, *Addendum 2 to Army Structure (ARSTRUC) Memorandum 2020-2024* (Feb. 4, 2019).

representatives in the Deputy Chief of Staff G-3/5/7 and the G-8.[12] At Army Futures Command, we met with representatives of the Army Futures and Concepts Center, including the officials who wrote the Army's multi-domain-related concepts.[13] Within TRADOC, we spoke with officials at the Combined Arms Center who focused on doctrine development and training, as well as the Force Development Directorate, the Fires Center of Excellence, and the Cyber Center of Excellence. We also spoke with members of the Army's Cyber Protection Brigade, Joint Force Headquarters-Cyber, and members of U.S. Army Pacific.

To address our second objective, we reviewed Army doctrine related to overall operations, cyber operations, and fires. We reviewed force structure documents, such as force design updates, Army Structure Memorandums, and other associated briefings related to planned changes, as well as changes being considered for the future. We spoke with Army headquarters officials in charge of building new cyber units, as well as officials at Army Futures Command and TRADOC. We compared the Army's process for establishing new cyber and electronic warfare units with the Army guidance and the *Standards for Internal Control in the Federal Government*.[14]

To address our third objective, we reviewed Army white papers and concept documents related to multi-domain operations, including the new Army Operating Concept published in December 2018—TRADOC Pamphlet 525-3-1: *The U.S. Army in Multi-Domain Operations 2028*—as well as related concepts and papers from the Joint Staff and other

[12]The Department of the Army headquarters Deputy Chief of Staff G-3/5/7 office has several responsibilities including developing and implementing Army policies for managing and structuring the Army, training military and civilian personnel, and advising on cyber, electronic warfare, and space operations not otherwise assigned by law, regulation, or policy. The Department of the Army headquarters G-8 office validates, approves, and prioritizes Army materiel capabilities and ensures the integration of materiel capabilities across mission and functional areas. See Headquarters, Department of the Army General Orders No. 2019-01, *Assignment of Functions and Responsibilities within Headquarters, Department of the Army* (May 15, 2019).

[13]The Army Futures and Concepts Center was formerly the Army Capabilities Integration Center under the authority of TRADOC. Authority for the Army Capabilities Integration Center officially transferred to Army Futures Command on Dec. 7, 2018, and the name was changed.

[14]Army Pamphlet 71-32, *Force Development and Documentation Consolidated Procedures* (Mar. 21, 2019). Also GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

services addressing multi-domain operations. We reviewed Army and Joint Staff guidance on developing concepts to understand existing requirements and frameworks for inter-service and Joint Staff collaboration on the development of concepts. We also reviewed other documentation for evidence of collaboration between the Army and the Joint Staff and other services, such as working group meetings, after-action reports on tabletop exercises, and agreements. We also met with Army officials, including officials from Army headquarters and TRADOC, to determine how the Army is developing its concept, and with Joint Staff and other services' officials, including J-7 Joint Concept Development, Air Force Air Combat Command, Marine Corps Futures Directorate, and U.S. Navy Fleet Forces, to understand the degree of collaboration, as well as current challenges and plans for developing multi-domain concepts. We discussed the results of our assessment with the Joint Staff and officials from the military services.

We conducted this performance audit from December 2017 to August 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

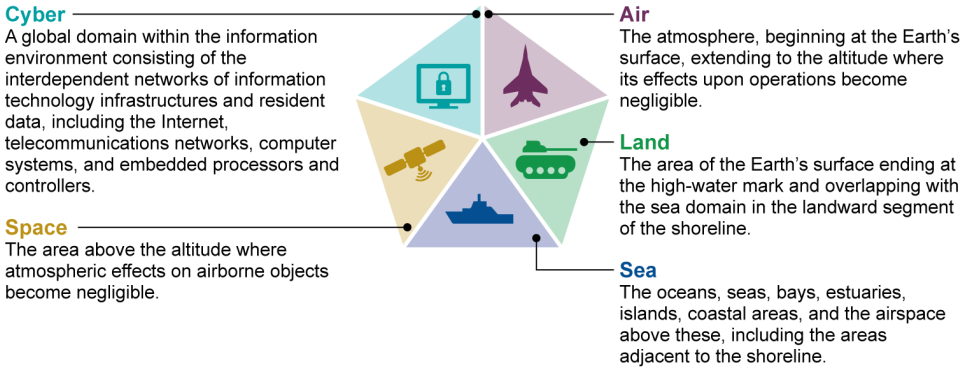
Background

Changing Warfare Environment

According to the *Summary of the 2018 National Defense Strategy* and the Army, the character of warfare is changing.[15] For decades, the United States enjoyed uncontested or dominant superiority in every operating domain—land, air, sea, cyber, and space—but today every domain is likely to be contested by other great-power competitors and potential regional adversaries. Figure 1 below describes these operating domains.

[15]DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Jan. 19, 2018).

Figure 1: The Five Warfighting Domains Envisioned by the Army Operating Concept



Source: GAO analysis of Department of Defense information. | GAO-19-570

Since at least 2012, DOD began shifting its focus from counterinsurgency operations in Iraq and Afghanistan to adversaries who possess more sophisticated capabilities. For example:

- In 2012, DOD issued strategic guidance that cited efforts by Iran and China to pursue cyber and electronic warfare capabilities with the ability to counter U.S. power projection and limit operational access.[16]
- The 2014 Quadrennial Defense Review acknowledged the efforts of China and others to counter U.S. strengths using anti-access and area-denial approaches and using new cyber and space control technologies.[17] The 2014 Quadrennial Defense Review also addressed the rapid evolution of modern warfare, including increasingly contested battlespaces in the air, sea, space and cyber domains.

[16]DOD, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, D.C.: January 2012).

[17]DOD, *Quadrennial Defense Review 2014* (Washington, D.C.: Mar. 4, 2014). Anti-access and area-denial strategies and capabilities are designed to either prevent an opposing force from entering an operational area (anti-access) or limit an opposing force's freedom of action within an operational area (area-denial). See GAO, *Defense Planning: DOD Needs Specific Measures and Milestones to Gauge Progress of Preparations for Operational Access Challenges*, GAO-14-801 (Washington, D.C.: Sept. 10, 2014). We found that DOD's plan for implementing the Joint Operational Access Concept did not contain measures and milestones to gauge progress and recommended that future iterations of the implementation plan include those measures and milestones. DOD concurred and implemented the recommendation.

- In 2016, an Army study of Russia's operations and doctrine concluded that Russia employs formations, operational concepts, and capabilities that overmatch U.S. capabilities in range and lethality, thus challenging the Army's ability to conduct operations and win battles.

The 2017 National Security Strategy stated that U.S. advantages are shrinking as rival states modernize their forces.[18] The 2017 National Security Strategy identified many of the challenges that China and Russia pose, including Russia's use of offensive cyber efforts to influence public opinion, and how cyberattacks have become a key feature of modern warfare. A classified National Defense Strategy followed in January 2018, and the unclassified summary cited challenges to the U.S. military advantage as a shift in the global environment.[19]

Purpose and Origins of the Multi-Domain Operations Concept

The Army's multi-domain operations concept originates from an Army effort to rethink how it will fight in the new, more complex operating environment. The Army defines multi-domain operations as ways for confronting adversaries in contested environments by presenting them with multiple challenges through the combining of multiple capabilities. This means that ground forces should be able to operate freely in other warfighting domains and, if necessary, be able to overwhelm an adversary's forces by combining capabilities across different domains, such as land, air, sea, cyber, and space simultaneously.

According to Army officials, in 2014 the then-Deputy Secretary of Defense tasked the Army to update its warfighting concept to deal with the threats and challenges posed by great-power competitors in the future operating environment. The Army officials added that around the same time, the Army began developing and running a wargame scenario focused on a threat that employed similar doctrine, tactics, and capabilities as those used by Russia in Ukraine. In 2016, the Army also assessed the increasingly sophisticated Russian military capabilities and identified specific multi-domain challenges that the Army would face if it came into conflict with Russia. Army officials said that its analysis highlighted the urgency of updating how it would fight such an adversary. In beginning to

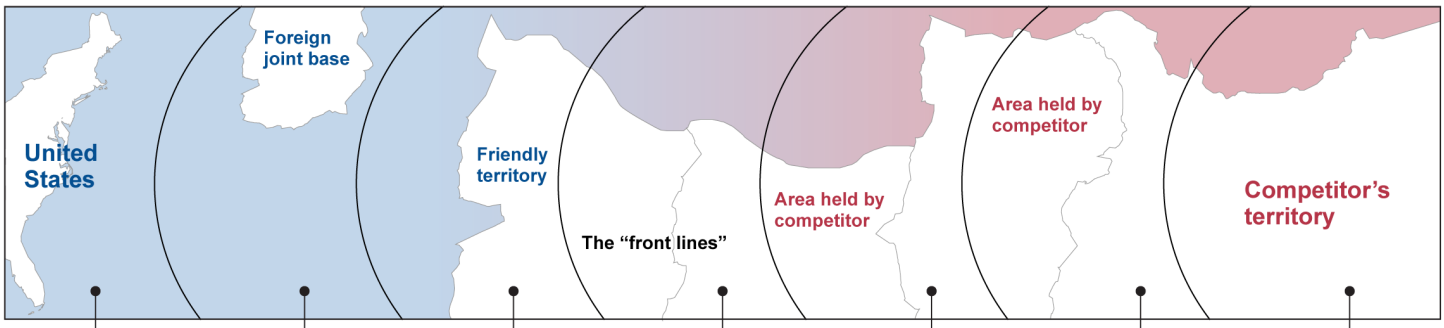
[18]*National Security Strategy of the United States of America* (Washington, D.C.: December 2017).

[19]DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Jan. 19, 2018).

develop this concept, the Army reached out to the Marine Corps, as both services face similar problems in ground-combat operations.

Since the Army began developing its concept, the Army established a framework for assessing how the adversary operates and the problems the Army needs to resolve as a ground force. For example, early on the Army developed an expanded battlefield that stretches far beyond the front lines, or “close area”, where ground forces face off against each other. Under this expanded battlefield, adversaries can use more sophisticated weapons and cyber capabilities that are based in distant and protected territories, potentially reaching targets that are located well behind the front lines, even within the continental United States. Figure 2 below depicts the Army’s new expanded battlefield for multi-domain operations, including a description of each area of the battlefield.

Figure 2: The Army's Expanded Battlefield in Multi-Domain Operations



Strategic Support Area
Extends from a theater of operations to the United States, or another combatant commander's area of responsibility, and includes the air and seaports supporting the flow of forces into the theater. Most friendly space and cyber capabilities are controlled from here. Assumed to be under surveillance at all times and targeted by long-range cyber and strike capabilities.

Operations Support Area
Friendly-held area where many key Joint Force command and control, sustainment, and air-or-sea-based strike capabilities are located. This area normally encompasses many entire nations; assumed to be targeted by enemy reconnaissance, information warfare, and long-range strike capabilities.

Tactical Support Area
Area held by friendly forces that directly enables military operations by providing sustainment, artillery, and command and control. Friendly units must be able to endure enemy information warfare, unconventional warfare, and artillery, and defeat infiltrating enemy ground forces.

Close Area
Friendly and enemy formations are in imminent physical contact. A commander's ability to take advantage of multi-domain effects from formations away from the battle is limited due to the immediacy of combat.

Deep Maneuver Area
Highly contested area held by a competitor where friendly ground forces can operate, but commanders must make a concerted effort to do so. Ground operations require significant support from air, cyber, and space domains. Generally, the objectives of an offensive military campaign lie within this area.

Operational Deep Fires Area
Territory held by a competitor that is potentially targetable by friendly artillery, air strikes, space and cyber capabilities. Operations here may seek to disrupt the enemy's operational reserves or prevent long-range cannon, rocket, or missile fires. Only friendly special operations ground forces operate here.

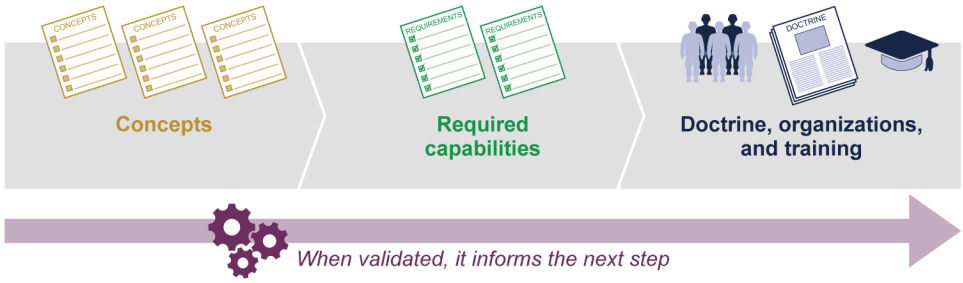
Strategic Deep Fires Area
A competitor's home base, generally unreachable by friendly ground forces due to geography or policy (e.g., on the other side of an international border). Potentially targetable by space and cyber capabilities.

Source: GAO analysis of Department of Defense information. | GAO-19-570

The Army Is Changing Its Doctrine, Organizations, and Training to Execute Multi-Domain Operations

The Army is changing aspects of its doctrine, organizations, and training simultaneously to develop a force that can effectively engage great-power competitors, such as Russia and China, across multiple domains, and expects this process to continue through the 2020s. Army concepts propose new approaches for the Army to develop capabilities against emerging challenges. The new Army Operating Concept built around multi-domain operations is intended to drive capability development, which is addressed through changes to the Army's doctrine, organizations, and training, among other areas. The Army's goal is to field a more lethal and capable force by 2028 that is able to dominate adversaries in a multi-domain environment.[20] Figure 3 below summarizes how the Army uses validated concepts to drive changes in capabilities and the force.

Figure 3: Concepts Shape Army Doctrine, Organizations, and Training



Source: GAO analysis of Army information. | GAO-19-570

Doctrine. Given the Army's attention to multi-domain operations, it has updated or is in the process of updating doctrine that guides how the Army fights. Primary among this effort is updating the Army's overarching operations field manual, which establishes how the Army conducts large-scale ground combat operations against the threat posed by a great-power competitor, among other things.[21] In its most recent revision to its doctrine, the Army incorporated several aspects of multi-domain operations, such as the expanded battlefield that includes cyber and the electromagnetic spectrum. TRADOC officials stated that they are also in

[20]Department of the Army, *The Army Strategy* (October 2018).

[21]Department of the Army, *Field Manual 3-0, Operations* (Dec. 6, 2017). According to Army officials, the doctrinal term has since changed from "large-scale ground combat operations" to "large-scale combat operations" to recognize the fact that in a close fight the Army will have to fight in more than the land domain.

the process of updating doctrine related to cyber operations and field artillery operations in order to build a force that can integrate both cyber capabilities and long-range fires—such as artillery, rockets, and missiles—for multi-domain operations.[22] The officials added that the Army is developing or is planning to develop specific doctrinal guidance for new Army units that will focus on multi-domain operations in the areas of intelligence, cyber, electronic warfare, and space.

Organizations. The Army wants to ensure that its warfighting organizations have the engineering, artillery, air defense, and other enabling capabilities needed to conduct multi-domain operations. For example, the Army believes that formations above the brigade level, such as division headquarters and corps headquarters, must have the ability to conduct electronic warfare and cyber operations. To that end, the Army is creating several new organizations focused on cyber and electronic warfare (discussed later in the report). Additionally, the Army is trying to align its multi-domain operations concept with a complementary concept focused on the roles and responsibilities of these organizations above the brigade level.[23] Expanding the roles and responsibilities of formations above the brigade level signifies a departure from the Army's modular force, which was implemented beginning in 2004. At that time, the Army embedded "key enablers" such as military intelligence, reconnaissance, and logistics functions, as well as other specialized personnel and equipment, into brigade combat teams to provide them independent capabilities.[24] Moving forward, the Army envisions enhancing the capabilities of brigade combat teams for multi-domain operations, as well as providing additional key capabilities to formations above the brigade level. For example:

[22]Department of the Army, *Field Manual 3-12, Cyberspace and Electronic Warfare Operations* (Apr. 11, 2017). Also, *Field Manual 3-09, Field Artillery Operations and Fire Support* (Apr. 4, 2014).

[23]Department of the Army, *The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (Sept. 24, 2018).

[24]We last reported on the Army's modular force transformation in 2014. See GAO, *Army Modular Force Structure: Annual Report Generally Met Requirements, but Challenges in Estimating Costs and Assessing Capability Remain,* GAO-14-294, (Washington, D.C.: Apr. 16, 2014).

- *Brigade combat teams*. Brigade combat teams are the Army's primary tactical unit, composed of around 4,400-4,700 soldiers.[25] They are being adjusted to conduct operations in the cyber domain, including new platoons focused on electronic warfare.
- *Army division headquarters*. Army divisions command multiple brigade combat teams. The Army expects division headquarters to manage the electromagnetic spectrum and to be the primary echelon for integrating aviation, fires, and electronic warfare into ground maneuver to defeat enemies in a close fight.
- *Army corps headquarters*. Army corps command multiple divisions. Under the Army's concept, the Army corps headquarters will be the primary echelon for defeating mid- and long-range enemy artillery fires. The Army corps will also integrate artillery rockets and missiles, as well as cyber capabilities in support of division or brigade ground operations.
- *Field armies*. Field armies, which have the ability to command two or more Army corps, are forward-stationed in regions with capable threats posed by great-power competitors. They will conduct campaigns to compete with adversaries short of armed conflict, and manage the transition to armed conflict should it be needed. The field army will also direct deception operations and provide long-range artillery and fires support.[26]
- *Theater armies*. Theater armies are also forward-stationed forces and will be responsible for managing and combining Army capabilities in support of information environment operations and space operations.[27] The theater army must be able to protect joint bases and networks and enable access to the theater.

[25]The size of the brigade combat team depends on whether it is an armored brigade combat team, an infantry brigade combat team, or a Stryker brigade combat team.

[26]Military deception is actions executed to deliberately mislead adversary military, paramilitary, and violent extremist organization decision makers, thereby causing the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission. See DOD, *Joint Publication 3-13.4: Military Deception* (Feb. 14, 2017).

[27]DOD defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Information operations are the integrated employment, during military operations of information-related capabilities along with other lines of operation, to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. See DOD, *Strategy for Operations in the Information Environment* (June 2016).

Training. The Army is also updating its training across a broad range of efforts. Army training officials stated that there is a need to train units collectively under multi-domain operations conditions against great-power competitors like Russia and China, per guidance from the Chief of Staff of the Army. The commander of Army Forces Command also issued guidance for fiscal year 2019 to help train and prepare soldiers to conduct multi-domain operations.[28] This guidance included increasing the realism and rigor of every unit rotation to one of the Army's combat training centers, as well as designing warfighter exercises that focus on units conducting operations in contested electronic warfare, cyber, and space environments. Additionally, the training officials stated that in recent years the Army has updated its decisive-action training scenarios to include regional versions for Europe, the Pacific, and Africa that comply with the multi-domain operations concept.[29] The officials added that, in future years, several Army organizations will be collaborating to modernize the Army's home-station training and combat training centers in support of fielding a force capable of conducting multi-domain operations.[30] All of this builds upon the Army's earlier efforts to shift its training focus to large-scale combat after a decade of training for counterinsurgency operations, as we testified to Congress in February 2019.[31]

The Army is also taking steps to revise the training for cyber and electronic warfare personnel. These steps include revising the *U.S. Army Cyberspace Operations Training Strategy* so that it accounts for new equipment and doctrine, but also for the new organizations being created and the tasks those units will be expected to perform, according to Army cyber officials.[32] Additionally, the Army Cyber School is revising its cyber and electronic warfare training so that personnel will be able to conduct

[28]Department of the Army, Headquarters United States Army Forces Command, *FORSCOM Command Training Guidance (CTG)—Fiscal Year 2019 (FY19)*, Memorandum for Headquarters, Commands Reporting Directly to FORSCOM (Fort Bragg, N.C.: Aug. 7, 2018).

[29]Decisive-action training is training to execute continuous and simultaneous combinations of offensive, defensive, and stability or defense support to civil authority tasks. See Army, *Field Manual 3-96, Brigade Combat Team* (Oct. 8, 2015).

[30]Training at the combat training centers focuses on Army functions such as *maneuver* and *mission command*.

[31]GAO-19-367T.

[32]Department of the Army, *U.S. Army Cyberspace Operations Training Strategy* (Washington, D.C.: Aug. 7, 2017).

multi-domain operations. Furthermore, the Army is working on a joint solution for training cyber personnel on behalf of U.S. Cyber Command, according to Army Cyber Command officials.[33] The Army's goal is to provide the total cyber force with the ability to conduct joint cyber training, including exercises and mission rehearsals by developing a virtual training environment that simulates realistic cyber threats. This cyber training solution, called the Persistent Cyber Training Environment, will allow for experimentation, unit certification, and assessment and development of the cyber mission force in a virtual training environment. The Army's goal is that the environment will decrease training time, increase throughput of personnel, and improve training quality. One of the stated operational imperatives of the Persistent Cyber Training Environment is to become integrated with multi-domain exercises.

[33]GAO, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, D.C.: Mar. 6, 2019). We reported on the efforts of U.S. Cyber Command and the services to train and maintain forces for key cyber missions. U.S. Cyber Command is a unified combatant command focused on cyber operations.

The Army Is Establishing New Cyber and Electronic Warfare Units, but Units Are Facing Staff, Equipment, and Training Shortfalls in Part Due to Incomplete Risk Assessments

The Army Is Activating Several New Cyber and Electronic Warfare Units at an Accelerated Pace and Is Facing Challenges

The Army is seeking to quickly create or design several new cyber and electronic warfare units in order to execute multi-domain operations; however, Army leadership is activating some units at an accelerated pace due to the sense of urgency imposed by the growing capabilities of potential great-power competitors. Some of these new Army units are more narrowly focused on a particular domain or skill set, such as the recently activated 915th Cyber Warfare Support Battalion based out of Fort Gordon, Georgia, and new Electronic Warfare Companies and platoons. The 915th Cyber Warfare Support Battalion will focus on providing offensive cyber capabilities consistent with its authorities to conduct offensive operations. The battalion is designed to fit with various Army formations—such as corps, divisions, or brigade combat teams—as assigned by the Army. The Electronic Warfare Companies, which are scheduled to be fielded during fiscal years 2023 through 2025 according to Army officials, will be attached to an Army corps and will be capable of planning and conducting electronic warfare operations. Electronic Warfare platoons, which Army officials said are scheduled to be fielded during fiscal years 2020 through 2022, will provide similar capabilities to brigade combat teams and other Army tactical-level formations.

Other units are being designed to plan and conduct operations in and across multiple domains, with specialists in cyber, electronic warfare, space, and intelligence assigned to the same unit. For example, a recently activated Intelligence, Cyber, Electronic Warfare, and Space (ICEWS) unit will be capable of planning and directing operations in any

or all of those areas. The ICEWS unit will function as part of a larger Multi-Domain Task Force, which will be capable of expanding those operations into other domains such as land and air. The Army plans to field at least two of these ICEWS units by the end of fiscal year 2020. Additionally, the Army is restructuring or creating Cyber, Electromagnetic Activities planning sections in the headquarters of more than 125 Army formations, from special forces units up to theater-level Army headquarters. This restructuring effort will take place during fiscal years 2020 through 2022, according to Army officials.

Army guidance states that a unit's activation date should be identified 1 to 2 years in advance, according to Army officials, in order to provide time to build up trained personnel and equipment in the unit before it is activated and available to be deployed.[34] As a result of accelerating the activation of these units, the Army is facing interrelated challenges in terms of staffing, equipping, and training the units, as discussed below.[35]

Accelerated pace creates challenges filling positions. The Army has had difficulty filling its ICEWS unit and the 915th Cyber Warfare Support Battalion with personnel to conduct operations. See table 1 below.

Table 1: The Army Is Activating New Units at an Accelerated Pace Resulting in Staff Shortages as of March 2019

	Authorized staff positions	Number of personnel in unit	Percentage of positions filled
Intelligence, Cyber, Electronic Warfare, and Space unit	199	110	55
915th Cyber Warfare Support Battalion	171	30	18

Source: DOD officials and GAO analysis of DOD information. I GAO-19-570

By accelerating the activation of the ICEWS unit in October 2018 as a pilot, or test, program, the Army activated the unit with only 32 percent of

[34]Department of the Army, *Army Regulation 71-32: Force Development and Documentation Consolidated Policies* (March 20, 2019).

[35]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018). We have reported on challenges related to personnel (recruiting, hiring, and retaining cyber security personnel), equipping (supply chain issues), and training (identifying the needed skills) across the federal government.

its personnel in place, and Army headquarters officials report that filling the unit with personnel with the right skills has been a slow process. The 915th Cyber Warfare Support Battalion is facing similar staffing challenges. As of the end of March 2019, the unit was understaffed by more than 80 percent as it filled 30 of 171 authorized positions for fiscal year 2019, according to an Army headquarters official. The official acknowledged that the 915th Cyber Warfare Support Battalion may not meet the authorized staffing levels for fiscal year 2019 if higher priorities arise for the service.

Looking ahead, Army officials said that filling all of these new cyber and electronic warfare units could be challenging because cyber personnel are in high demand, with competition for these skilled personnel existing between the Army, other government entities, and the private sector. Army headquarters officials said they are exploring options to address the challenges and have taken steps to retain the personnel that they have, mostly in the form of retention bonuses and incentive pay. Some of those incentives are targeted at the senior enlisted levels, which are some of the personnel that Army officials indicated are in the most demand and of which they have a shortage.

Accelerated pace creates equipping challenges. Officials with both Army headquarters and the Army Cyber School cited equipment challenges as one of the key issues that must be addressed when activating a unit on an accelerated basis. For example, in November 2018, an Army headquarters' official responsible for building the ICEWS unit stated that the Army was having a difficult time identifying where the unit's equipment would be coming from. By the end of January 2019, the official said the situation was improving and that 55 percent of the equipment had been identified, but the Army was trying to find a source for the remaining 45 percent. However, most of this is common Army equipment, such as firearms, according to an Army official; those percentages do not include the specialized cyber equipment that the unit will need to perform its missions, such as a communications system designed to transfer data beyond the line of sight during air defense operations. An Army headquarters' official stated that the Army is prototyping different types of specialized equipment in order to expedite the acquisition of such capabilities.

Revisions to training not keeping up with activation of units. Army officials acknowledged the need to update its cyber training, in part because the doctrine for new units is still being written. Officials with the Army Cyber School and the Army's Combined Arms Center stated that

the current *U.S. Army Cyberspace Operations Training Strategy* did not foresee all of the new cyber and electronic warfare organizations the Army now intends to create, including the Cyber Electromagnetic Activities sections attached to various formations.[36] Army headquarters officials stated that they are working on a revision to the *U.S. Army Cyberspace Operations Training Strategy* to address these issues. However, the first ICEWS unit and the 915th Cyber Warfare Support Battalion were activated without this updated training strategy. With other units scheduled to be activated in fiscal year 2020, it is possible others may be activated without the training strategy as well. Without the updated doctrine and subsequent training strategies that will result from it, TRADOC officials said they would have difficulty designing training for the new units, and soldiers will not have a clear understanding of their tasks and missions.

Obtaining equipment also could be a challenge for training servicemembers before they are assigned to cyber or electronic warfare units, according to some Army officials. Officials with the Army Cyber School stated that it could end up growing and producing a workforce that outpaces its ability to procure equipment. However, Army headquarters' officials stated that equipping operational units is a higher priority than providing equipment to the schools for training, and the Army ensures that those units receiving the equipment get the training they need upon fielding the equipment. If the Army does not acquire new equipment quickly enough, the result could be that soldiers in the Army Cyber School will be trained on outdated equipment, which they will not use when they get to the field.

[36]Department of the Army, *U.S. Army Cyberspace Operations Training Strategy* (Washington, D.C.: Aug. 7, 2017).

The Army Assessed Staffing, Training, and Equipping Risks for Certain Cyber and Electronic Warfare Units, but Its Assessments for Units Activated at an Accelerated Pace Are Incomplete

In the process of creating some new units, the Army assessed the risk of whether it can meet the units' staffing, equipping, and training requirements before the units' activation date, but it did not do so for those units activated at an accelerated pace. For example, the Army conducted risk assessments for some new Electronic Warfare platoons and Cyber Electromagnetic Activities sections that it plans to begin activating in fiscal year 2020. Those assessments identified issues and mitigation strategies for the Army to consider when making fielding and resource decisions. For example, the risk of finding a sufficient number of qualified personnel for the Electronic Warfare platoons and Cyber Electromagnetic Activities sections would be mitigated by spreading the activations over a minimum of 3 years. The assessment for the Electronic Warfare platoons also identified some equipping issues that will require either more senior-level input or extending timeframes for completion.

In contrast, the Army activated the ICEWS unit and the 915th Cyber Warfare Support Battalion in an accelerated manner because of the urgent need to develop these organizations, given the growing capabilities of potential great-power competitors. However, the Army did so without completely assessing the staffing, equipping, and training risk to those units over the long term. For example:

- According to Army officials, the Army did not perform a risk assessment for the ICEWS unit currently assigned to and participating in exercises in the Pacific, because the Army initiated the unit as a pilot, or test, program. According to Army officials, a risk assessment was unnecessary prior to activating the unit because the Army expects to refine the unit's personnel, equipping, and training requirements during the pilot program. However, the ICEWS unit is expected to become part of a larger Multi-Domain Task Force in fiscal year 2020. Until that occurs, the ICEWS unit is attached to another active Army unit and, according to Army officials, eligible to be deployed if needed based on its current capabilities. Unless the Army assesses the staffing, equipping, and training risks of the ICEWS unit, the unit may be unable to provide the expected capabilities, either currently or as part of the larger task force to which it will belong.
- The Army performed an initial risk assessment for the 915th Cyber Warfare Support Battalion before the unit was activated in December 2018. However, Army officials told us that the Army has plans to grow the unit to as many as 627 personnel by 2024, at which point it would be considered fully operational. Unless the Army performs a more complete risk assessment of the 915th Cyber Warfare Support Battalion's staffing, equipping, and training requirements prior to

achieving full operational capability, the Army may be poorly positioned to make decisions about how to use and support the battalion.

Army guidance states that the Army should assess its ability to support a new unit's staffing, equipping, and training requirements, among other things, so that senior Army leaders can evaluate proposed organizational changes.[37] For example, under a force integration functional area analysis, the Army staff evaluates all proposed organizational changes to ensure that they meet the intent of senior Army leaders, have the resources available to accomplish their mission, and that their projected benefits justify increased resources.[38] These assessments analyze the proposed organization in nine areas, such as staffing, structuring, equipping, and training, and are intended to give senior Army leaders an understanding of whether the organizations are affordable, supportable, and sustainable.[39] According to Army officials, the force integration functional area analysis is similar to a risk assessment. In addition, *Standards for Internal Control in the Federal Government* state that management should identify, analyze, and respond to the risks related to achieving the defined objective—in this case quickly fielding a cyber force to deal with current threats.[40]

Because the Army has not completely assessed the risk of organizing the ICEWS unit and the 915th Cyber Warfare Support Battalion, senior Army leaders may be left with an incomplete picture of the challenges in

[37]Army Pamphlet 71-32, *Force Development and Documentation Consolidated Procedures* (March 21, 2019).

[38]According to Army Regulation 71-32, *Force Development and Documentation Consolidated Policies* (March 20, 2019), the Deputy Chief of Staff, G-3/5/7, is responsible for coordinating and supervising activities related to the development and management of the force to ensure synchronization of all force integration functional area analyses to support programmed activations, conversions, inactivations, or relocation actions.

[39]The nine functional areas are structuring, manning, equipping, training, sustaining, funding, deploying, stationing, and readiness.

[40]GAO-14-704G.

affording, supporting, and sustaining these units over the long term.[41] Moreover, senior Army leaders lacked key information needed to understand the capability and capacity of the units at the time they were activated. For example, these units currently do not have what they need in terms of personnel and equipment to conduct their missions successfully. Further, according to some Army officials, without such an assessment, the Army does not know whether accelerated activation was the best course of action; what challenges they may face in staffing, equipping, and training the units; or how to mitigate challenges that may arise in other areas, such as deploying and sustainment. Army officials stated that there is a lot of informal discussion between relevant Army offices to try to identify and deal with challenges for these units. However, they also acknowledged the problems inherent in activating a unit by accelerating timelines.

Such risk assessments also could inform future Army decisions as it activates new units for multi-domain operations. Given the Army's perception of the threat environment, the Army may decide to activate other multi-domain operations units in an accelerated manner. For example, the Army is exploring ideas for creating several new units in future years to enhance its capability in multi-domain operations, such as a Theater Space Warfare Battalion. The Army also has been running wargames to see how they would operate new types of units at the division, corps, and theater level for commanding and operating long-range missiles and rockets.

Army officials stated that as these units grow and evolve, it is uncertain when more comprehensive risk assessments would take place. If the Army does not perform a risk assessment for the activated ICEWS unit before it joins the larger Multi-Domain Task Force, or a more complete risk assessment for the 915th Cyber Warfare Support Battalion as that unit matures, the Army may end up fielding units that are not capable of

[41]In the past, when faced with a similar sense of urgency, the Army accelerated the activation of its first Security Force Assistance Brigade. In December 2018, we reported that unit was encountering similar challenges as those cited in this report for the ICEWS unit and the 915th Cyber Warfare Support Battalion. Specifically, we reported that an acceleration of the unit's activation and deployment timelines by at least 8 months resulted in several issues related to staffing and training the brigade and providing sufficient enabling force to support the brigade's mission. We did not make recommendations in the report. See GAO, *Security Force Assistance: U.S. Advising of Afghan National Army Has Expanded since 2015, and the U.S. Army Has Deployed a New Advising Unit,* GAO-19-251R (Washington, D.C.: Dec. 19, 2018).

providing the needed capabilities. Moreover, these risk assessments could provide vital lessons that could inform future Army decisions on the development, activation, and fielding of other units focused on enhancing the Army's capability to conduct multi-domain operations.

The Army Engaged with the Joint Staff and Other Services and Envisions Opportunities for Further Coordination

The Army engaged with the Joint Staff and other services to develop its Army Operating Concept and envisions opportunities for further coordination in the future. The Army's overarching objective is to field a multi-domain-capable force by 2028, and it considers further engagement with the Joint Staff and other services as essential to accomplishing that goal. According to Army plans, the Army needs to finalize the next version of its Army Operating Concept by the fall of 2019 in order to incorporate multi-domain operations into all levels of Army leadership, training, and education by 2020.[42] The Army plans indicate that maintaining this schedule is important to have a ready, lethal, and modern force for multi-domain operations by 2028.

From the outset, the Army engaged with the Marine Corps to begin its concept development. Together the Army and Marine Corps published a white paper in January 2017 where they unveiled "Multi-Domain Battle" as a new concept for combat operations against a sophisticated great-power competitor.[43] This white paper highlighted the need for ground forces to focus on all five warfighting domains and was intended as a first step toward further multi-domain concept development, wargaming, experimentation, and capability development.

Once the white paper was written, the Army engaged with the Joint Staff and the other services in several ways to refine its concept:

[42]Department of the Army, *The Army Strategy* (Washington, D.C.: 2018). The Army Strategy articulates how the total Army achieves its objectives defined by the Army Vision, namely: the Army of 2028 will be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere, in a joint, combined, multi-domain, high-intensity conflict, while simultaneously deterring others and maintaining its ability to conduct irregular warfare. The Army will do this through the employment of modern manned and unmanned ground-combat vehicles, aircraft, sustainment systems, and weapons, coupled with robust combined arms formations and tactics based on a modern warfighting doctrine, and centered on exceptional leaders and soldiers of unmatched lethality.

[43]United States Army-Marine Corps White Paper, *Multi-Domain Battle: Combined Arms for the 21st Century*, (Jan. 18, 2017).

- **Joint Staff collaboration**. The Army engaged with the Joint Staff on an Army-led study of recent contingency operations and used the lessons to refine the Army Operating Concept's description of the emerging operational environment. Based on that study, the Army also refined some solutions for addressing threats posed by great-power competitors. Joint Staff officials reported that the Army engaged with the Joint Staff through other collaborative events as well, including tabletop exercises that tested and refined multi-domain concept ideas.
- **Marine Corps collaboration**. As the Army moved forward from the white paper, the Marine Corps' input informed the concept's development in various ways. This included changing the concept's title from multi-domain battle to multi-domain operations in April 2018 to better reflect the scope of competition and conflict, as well as the inherent joint nature of modern warfare. The Marine Corps also hosted a multi-domain symposium in April 2018 that was attended by the Army, Air Force, Navy, and Joint Staff.
- **Air Force collaboration**. The Army initially collaborated with the Air Force Air Combat Command to inform concept-development efforts, and more recently began working with the Air Force Warfighting Integration Capability under Air Force headquarters. Also, the Army and Air Force collaborated on tabletop exercises focused on simulating multi-domain operations. Army officials told us that this helped them refine their thinking on how to enhance the maneuverability of its land forces by combining Army and Air Force capabilities across domains.
- **Navy collaboration**. The Army and Navy principally collaborated by testing multi-domain capabilities during real-world exercises. For example, the Army joined the Navy's 2018 Naval Rim of the Pacific exercise to demonstrate capabilities for multi-domain operations in a real world environment.

While the Army took steps to engage with the Joint Staff and the other services, it made the decision to move forward with the latest version of its Army Operating Concept in order to meet its overarching objective to develop a multi-domain operations-capable force by 2028. Given this urgency, Army officials told us that they may have missed opportunities to further refine its Army Operating Concept in 2018 with the perspectives of the Joint Staff and other military services. Joint Staff officials told us that by not fully including the Joint Staff in some tabletop exercises, the Army may have missed the Joint Staff's perspective on key issues related to multi-domain operations, such as joint command and control.

As the Army continues to revise its Army Operating Concept, the Army recognizes the need to continue to engage with the Joint Staff and other services. Joint Staff officials told us that the Joint Staff has initiated its own plans to engage with the services to refine key ideas of multi-domain operations in joint concepts, including logistics, intelligence, and command and control. Army officials told us that they recognize the importance of not getting too far ahead of these efforts, or the efforts of other services related to multi-domain operations. Army officials told us that the mechanisms built into the Joint concept-development framework would provide opportunities to engage the services and Joint Staff as the Army revises its own concept. Army officials added that beginning in the fall of 2019 the Army will participate with the Joint Staff in a wargame designed, in part, to analyze how the Army Operating Concept works with the other military service operating concepts. As a result, the current concepts are likely to evolve in the future as the Army synchronizes its efforts with those of the Joint Staff and other services.

Conclusions

Rising threats posed by great-power competitors, particularly China and Russia, prompted the Army to initiate a profound and fundamental transformation to the way it plans to fight. The refinement of the Army's Operating Concept is beginning to drive changes across the Army. The Army is making near-term changes by incorporating multi-domain operations into its doctrine, organizations, and training, which includes the accelerated creation of new cyber and electronic warfare units. However, these units are short of both people and equipment. While Army leadership believes that the urgency to confront threats justifies its decision to accelerate the development of those units, the Army did not assess the risks associated with staffing, equipping, and training its existing ICEWS unit prior to activation to determine whether it is affordable, supportable, and sustainable, and officials said it was uncertain when a more comprehensive assessment would take place. The Army plans to incorporate this unit into the first Multi-Domain Task Force by the end of Fiscal Year 2020, but in the meantime the unit could be deployed if needed. The Army did prepare a preliminary risk assessment for the 915th Cyber Warfare Support Battalion prior to activation, but it is unclear whether the Army will perform a more comprehensive risk assessment as the unit matures and nears full operational capability. For the units already activated, a risk assessment could benefit the Army by providing insights about the ability to deploy and sustain the units. It is important for the Army to assess its efforts before committing resources to activate new units. By formally assessing the risk of all new units activated in an accelerated manner, the Army will

have the key information its leaders need for making decisions related to the activation of those units and other related units going forward.

Recommendations for Executive Action

We are making the following three recommendations to the Secretary of the Army.

The Secretary of the Army should ensure that the Deputy Chief of Staff, G-3/5/7 assess the risk associated with staffing, equipping, and training the existing ICEWS unit prior to its incorporation into the first Multi-Domain Task Force in fiscal year 2020. (Recommendation 1)

The Secretary of the Army should ensure that the Deputy Chief of Staff, G-3/5/7 conduct a comprehensive risk assessment associated with staffing, equipping, and training the 915th Cyber Warfare Support Battalion prior to approving the expansion of the unit to its full operational capability. (Recommendation 2)

The Secretary of the Army should ensure that the Deputy Chief of Staff, G-3/5/7 assess the risk associated with staffing, equipping, and training of new units that it plans to activate in an accelerated manner for the purposes of conducting multi-domain operations, taking into consideration the assessments performed on the first activated ICEWS battalion and the 915th Cyber Warfare Support Battalion. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In its written comments, reproduced in appendix I, the Army partially concurred with the first two recommendations and concurred with the third recommendation.

The Army partially concurred with the first recommendation for it to conduct a risk assessment, such as a force integration functional area analysis, for the first activated ICEWS unit. The Army stated in its comments that it does not perform force integration functional area analyses for experimental or pilot organizations, and that because the first ICEWS was activated as a pilot, no such assessment was performed. The Army added that it would conduct a risk assessment at the conclusion of the pilot if and when the Army decides to establish such a unit. We met with Army officials to discuss their comments, during which they provided additional information and clarification regarding how they were assessing risks for the unit. Based on this information, we modified the report to reflect the Army's position that a risk assessment was

unnecessary prior to activating the unit because the Army plans on using the pilot period to determine the staffing, equipping, and training requirements for the unit. We also incorporated additional information on the status of the ICEWS unit. As a result, we clarified our recommendation to state that the Army should assess the risk associated with staffing, equipping, and training the existing ICEWS unit prior to its incorporation into the first Multi-Domain Task Force in fiscal year 2020. Army officials generally agreed with the revised recommendation. Moving forward, it will be important for the Army to implement this recommendation to ensure the ICEWS unit, which is active and eligible to be deployed, will be prepared to carry out its mission effectively.

The Army partially concurred with the second recommendation for it to conduct a risk assessment, such as a force integration functional area analysis, for the 915th Cyber Warfare Support Battalion. The Army stated in its comments that it does not perform force integration functional area analyses for force generating units such as the 915th Cyber Warfare Support Battalion. Instead, it develops a concept plan, which applies rigor and analysis to determine the most efficient and effective way of fielding a new unit. We met with Army officials to discuss their comments, during which they provided additional information related to assessing risks for the 915th Cyber Warfare Support Battalion. Specifically, Army officials said that prior to activating the battalion, leadership approved the battalion's concept plan, which included an initial risk assessment. We reviewed the concept plan for the battalion and found that the assessment only addressed the risk of not having the unit's capabilities activated and in the field for operations. We incorporated this additional information on this initial risk assessment for the 915th Cyber Warfare Support Battalion into the report. As a result of this additional information, we clarified our recommendation to state that the Army should conduct a comprehensive risk assessment associated with staffing, equipping, and training the 915th Cyber Warfare Support Battalion prior to approving the expansion of the unit to its full operational capability. Army officials generally agreed with this. It will be important for the Army to implement the revised recommendation to ensure the 915th Cyber Warfare Support Battalion, which is active and performing operations, will be prepared to carry out its mission effectively.

The Army concurred with the third recommendation for it to ensure that a risk assessment is conducted before activating any new organizations it plans to field in an accelerated manner for the purposes of conducting multi-domain operations. The Army added that any lessons learned from the activation of the first ICEWS unit and the 915th Cyber Warfare

Support Battalion will be taken into consideration when assessing the risk before the activation of these new organizations. It will be important for the Army to implement the recommendation to ensure that any new organizations are prepared to carry out their missions, while potentially avoiding some of the challenges that the ICEWS and 915th Cyber Warfare Support Battalion have experienced.

Lastly, the Army also recommended that we change the title of our report; however, we did not accept the title offered by the Army. We believe the title accurately reflects the issues and recommendations highlighted in the report.

We are sending copies of this report to the appropriate congressional committees and to the Secretary of Defense; the Acting Under Secretary of Defense for Personnel and Readiness; the Chairman of the Joint Chiefs of Staff; the Acting Secretaries of the Departments of the Air Force and the Army; the Secretary of the Navy; and the Chief of Staff of the Army. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3489 or pendletonj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Staff members making key contributions to this report are listed in appendix II.

John H. Pendleton, Director
Defense Capabilities and Management

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Shelby
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Comments from the Department of the Army

DEPARTMENT OF THE ARMY
Office of the Deputy Chief of Staff, G-3/5/7
400 Army Pentagon
Washington, DC 20310-0400

AUG 0 1 2019

Mr. John Pendleton
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Pendleton,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-19-570SU, "FORCE STRUCTURE: Army Needs to Conduct Risk Assessments as it Expands its Warfighting Capabilities," dated June 4, 2019 (GAO Code 102419).

Attached is DoD's proposed response to the subject report. My point of contact is Mr. Gregory Wick who can be reached at gregory.j.wick.civ@mail.mil and phone (703) 693-2979.

Sincerely,

PETER N. BENCHOFF
Brigadier General, U.S. Army
Director, Force Management

Enclosure

GAO DRAFT REPORT DATED JUNE 4, 2019
GAO-19-570SU (GAO CODE 102419)

"FORCE STRUCTURE: ARMY NEEDS TO CONDUCT RISK ASSESSMENTS AS IT EXPANDS ITS WARFIGHTING CAPABILITIES"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of the Army should ensure that the Deputy Chief of Staff, G3/5/7 conduct a risk assessment, such as a Force Integration Functional Area analysis, for the first activated Intelligence, Cyber, Electronic Warfare, and Space (ICEWS) unit.

DoD RESPONSE: Partially concur. The Army does not conduct formal risk assessments for experimental or "pilot" units. The Army will conduct a risk assessment, such as a Force Integration Functional Area (FIFA) analysis, at the conclusion of the pilot, if and when the Army decides to establish such a unit. As stated in the draft report, the first ICEWS was activated as a pilot to test multi-domain task force concepts in the Indo-Pacific region. Its participation in exercises was intended to provide insights into future ICEWS organizational design decisions. Because the first ICEWS was a pilot organization, no FIFA-like assessment was done prior to its activation for experimentation.

RECOMMENDATION 2: The GAO recommends that the Secretary of the Army should ensure that the Deputy Chief of Staff, G3/5/7 conduct a risk assessment, such as a Force Integration Functional Area analysis, for the 915th Cyber Warfare Support Battalion (CWSB).

DoD RESPONSE: Partially concur. The Army does not conduct FIFA risk assessments for force generating units such as the 915th CWSB. However, the Army does develop "concept plans" to determine the most efficient and effective plan to field a new generating force unit. Concept plans apply rigor and analysis in the same way that FIFA analysis does for pilot organizations. The Army Director of Force Management approved a concept plan for the establishment of the CWSB unit in July 2018. The concept plan included 171 military authorizations out of a total of 627 requirements. The Army made the decision to grow the unit over several years to be able to assign newly trained personnel in the cyber career field to a unit, rather than assign them to other units until the aggregate personnel strength across the force totaled enough to establish the 915th at an initial high personnel fill level.

RECOMMENDATION 3: The GAO recommends that the Secretary of the Army should ensure that the Deputy Chief of Staff, G3/5/7 conduct a risk assessment, such as a FIFA analysis, before activating any new organization it plans to field in an accelerated manner for the purposes of conducting multi-domain operations, taking into consideration the assessments performed on the first activated ICEWS battalion and the 915th Cyber Warfare Support Battalion.

DoD RESPONSE: Concur. DCS, G-3/5/7 will ensure that a risk assessment, such as a FIFA, is conducted before activating any new organizations it plans to field in an accelerated manner for the purposes of conducting multi-domain operations. If applicable, any lessons learned from the

activation of the first ICEWS and the 915th CWSB will be taken into consideration when assessing risk before the activation of these new organizations.
ADDITIONAL COMMENTS

Recommend that the report be entitled: "FORCE STRUCTURE: Taking Measures to Improve Army Risk Assessments during the Rapid Standup of Expanded Warfighting Capabilities." The title of the draft report could be improved. The proposed title better captures both the intended outcome of the audit and the Army's commitment to improve risk assessment processes.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

John H. Pendleton, (202) 512-3489 or pendletonj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kevin O'Neill (Assistant Director), Matt Spiers (Analyst-in-Charge), Tracy Barnes, Shannon Finnegan, Christopher Gezon, Ruben Gzirian, J. Kristopher Keener, Alberto Leff, Joshua Leiling, Amie Lesser, Jon Ludwigson, Ned Malone, and Clarice Ransom made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.