INSPECTOR GENERAL

U.S. Department of Defense

FISCAL YEAR 2021

TOP DOD MANAGEMENT CHALLENGES

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Mission

To detect and deter fraud, waste, and abuse in Department of Defense programs and operations;

Promote the economy, efficiency, and effectiveness of the DoD; and

Help ensure ethical conduct throughout the DoD

Vision

Engaged oversight professionals dedicated to improving the DoD

For more information about whistleblower protection, please see the inside back cover.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

October 15, 2020

Each Inspector General (IG) is required by the Reports Consolidation Act of 2000 to prepare an annual statement summarizing what the IG considers to be the "most serious management and performance challenges facing the agency" and to assess the agency's progress in addressing those challenges. According to the law, each "agency head may comment on the IG's statement, but may not modify the statement." The IG's statement must be included in the Agency Financial Report.

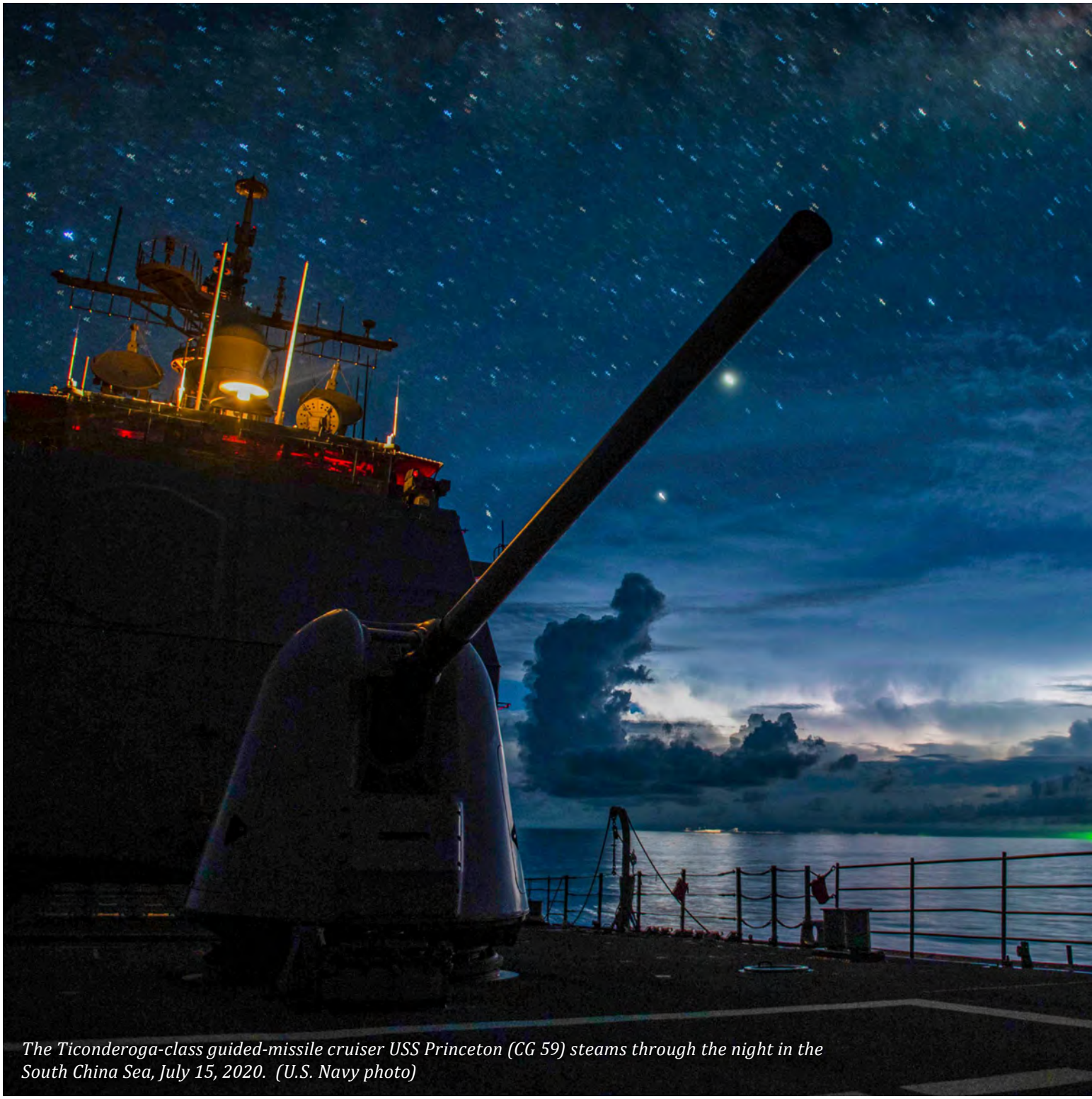
The DoD Office of Inspector General (OIG) independently identifies these challenges based on a variety of factors, including our independent research, assessment, and judgment; previous oversight work completed by the DoD OIG and other oversight organizations; congressional hearings and legislation; input from DoD officials; and issues highlighted by the media that are adversely affecting the DoD's ability to accomplish its mission.

While some of the challenges remain from prior years, the DoD OIG identified three new challenges this year. The new challenges are related to building and sustaining the DoD's technological dominance; non-traditional threats such as pandemics and extreme weather events; and transforming data into information. The remaining challenges have been identified in prior years, and the DoD has been working to resolve or mitigate the challenge areas. We also discuss the recent actions taken by the DoD to address these challenges; cite planned, ongoing, and completed oversight work related to the challenges; and assess the DoD's progress in each challenge area.

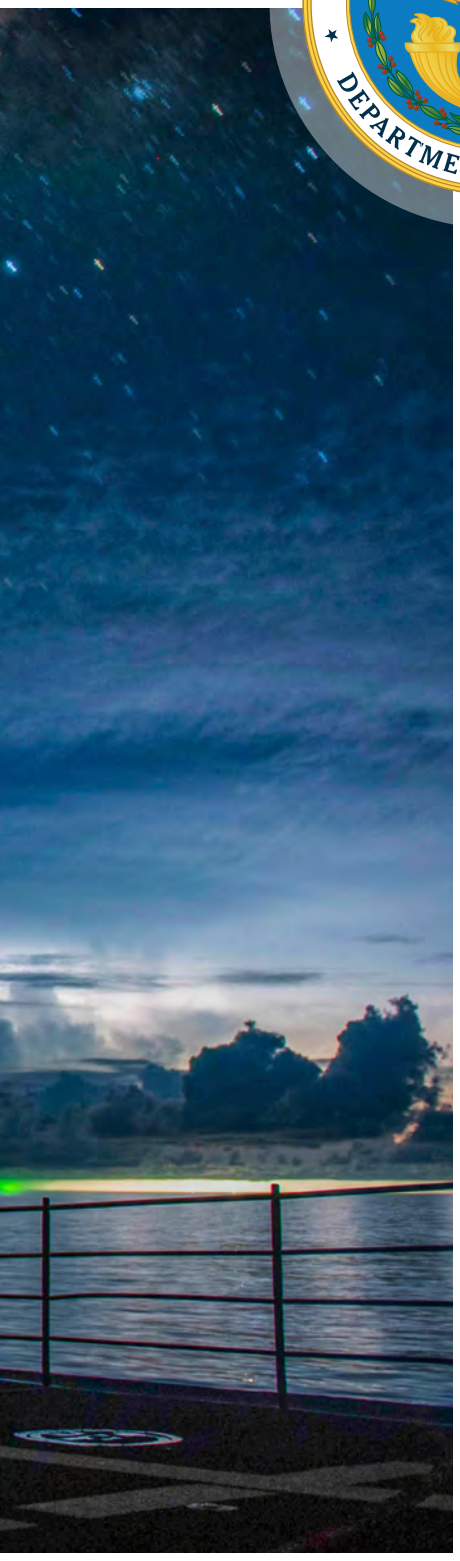
This document is forward-looking. The DoD OIG uses this document in its internal oversight planning process, seeking to ensure the DoD OIG's projects address the most significant performance and management challenges. These challenges are not listed in order of importance or by magnitude. All are critically important challenges facing the DoD.

The DoD OIG will continue to assess these challenges and conduct independent oversight to help promote the economy, efficiency, and effectiveness of the DoD; detect and deter fraud, waste, and abuse in DoD programs and operations; and ensure ethical conduct throughout the DoD. We look forward to working with the DoD to help address these important challenges.

Sean O'Donnell
Acting Inspector General



The Ticonderoga-class guided-missile cruiser USS Princeton (CG 59) steams through the night in the South China Sea, July 15, 2020. (U.S. Navy photo)



Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2021

U.S. Air Force weapons load crew members, assigned to the 58th Aircraft Maintenance Unit, load an advanced medium-range air-to-air missile (AMRAAM) to an F-35 Lightning II during Exercise Combat Archer at Eglin Air Force Base, Florida, June 10, 2020. (U.S. Air Force photo)

Executive Summary

The DoD OIG annually identifies the top management and performance challenges impacting the DoD, based upon solicitation of the DoD's input, reviewing congressional hearings and legislation, assessing oversight work by the U.S. Government Accountability Office and the DoD oversight community, and considering issues raised by media coverage. The DoD OIG also considers the DoD's progress in addressing these challenges. This report provides Congress and the DoD's civilian and military leaders an independent assessment of the management and performance challenges confronting the DoD.

FY 2021 TOP DOD MANAGEMENT CHALLENGES

The FY 2021 Top DoD Management Challenges are:

1. Maintaining the Advantage While Balancing Great Power Competition and Countering Global Terrorism
2. Building and Sustaining the DoD's Technological Dominance
3. Strengthening Resiliency to Non-Traditional Threats
4. Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense
5. Enhancing Cyberspace Operations and Capabilities and Securing the DoD's Information Systems, Network, and Data
6. Transforming Data Into a Strategic Asset
7. Ensuring Health and Safety of Military Personnel, Retirees, and Their Families
8. Strengthening and Securing the DoD Supply Chain and Defense Industrial Base
9. Improving Financial Management and Budgeting
10. Promoting Ethical Conduct and Decision Making

The challenges are not listed in order of priority, importance, or magnitude. Each challenge is critical to ensuring the DoD meets its mission to provide combat-ready forces to defend the United States.

NEW DOD MANAGEMENT CHALLENGES

This year, the DoD OIG combined and refocused the two challenges from the FY 2020 Management Challenges on countering global terrorism and countering China, Russia, Iran, and North Korea. The DoD OIG added three new challenges focusing on sustaining the DoD's technological dominance through emerging technologies, strengthening the U.S. military's resiliency to non-traditional threats, and transforming data into information.

The first challenge, "Maintaining the Advantage While Balancing Great Power Competition and Countering Global Terrorism," highlights the DoD's challenge of reorienting its priorities and attention to countering China, Russia, Iran, and North Korea after nearly 20 years of focusing on combatting global terrorist organizations. These revisionist powers (China and Russia) and rogue nations (Iran and North Korea) pose different threats than terrorist organizations and require distinct strategies, capabilities, and operations. Maintaining the U.S. military's advantage while balancing great power competition and countering global terrorism requires the DoD to focus on enhancing interagency collaboration and rebuilding military capabilities that may have atrophied the past 20 years.

The second challenge, "Building and Sustaining the DoD's Technological Dominance," focuses on emerging technologies that the DoD and U.S. adversaries are pursuing. Emerging technologies, such as hypersonic weapons, microelectronics, artificial intelligence, 5G communications, and biotechnologies, present both significant opportunities and challenges because each could revolutionize the conduct of war. Autonomous intelligent machines and applications can rapidly accelerate the speed of decision making and action in time-critical operations, improve understanding of the battlespace, and enable new missions that were previously impossible. Rapidly developing, procuring, and deploying these new, innovative technologies will be critical for the DoD to secure and maintain its competitive advantage over adversaries and competitors pursuing the same technologies.

The third challenge, "Strengthening Resiliency to Non-Traditional Threats," recognizes the growing issues involving non-traditional threats, such as pandemics, extreme weather events, and the national security implications of a changing environment. Non-traditional threats impact the U.S. military's infrastructure, readiness, and personnel. Rising sea levels; extreme weather such as flooding, wildfires, or hurricanes; and a melting Arctic will require the DoD to consider the security, readiness, and financial implications of these non-traditional threats. The DoD must also identify how to mitigate the risks and costs to U.S. national security interests, military installations, and personnel.

The sixth challenge, "Transforming Data Into a Strategic Asset," highlights the importance of data and information as a strategic asset. The DoD is awash in data and faces challenges turning data into valuable information for decision makers at all levels within the Department. The DoD has thousands of operational systems, data centers, and servers, millions of computers and devices, and hundreds of thousands of commercial mobile devices. Furthermore, new data is generated in massive volumes and speed in today's world of interconnected devices, with an estimated 2.5 quintillion (or 2.5 billion billion) bytes of data created every day. Collecting, storing, protecting, and analyzing the data is essential for DoD leaders to have the vital information they need to make decisions.

ENDURING DOD MANAGEMENT CHALLENGES

The DoD faces enduring challenges that do not significantly change each year. Several challenges from the FY 2020 Top DoD Management Challenges are enduring, but the OIG merged several challenges. Although several topics within the merged challenges—such as fraud, acquisition reforms, or payments for health care services with limited or no cost controls—are not discussed in this year's challenges, the DoD OIG's oversight and investigative work continues in these areas.

The fourth management challenge, "Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense," highlights the DoD's challenges of investing in new capabilities in these areas while also sustaining legacy systems to protect U.S. national security interests. Near-peer competitors and rogue nations are investing in their own capabilities to protect their own interests and deter or defeat U.S. capabilities in space, nuclear deterrence, and missile defense. The DoD must balance establishing a new service, the U.S. Space Force, and transitioning personnel, authorities, and programs, while also protecting U.S. space assets and dominance. All three legs of the U.S. nuclear triad are rapidly approaching the end of their planned service lives, forcing the DoD to modernize aging systems without sacrificing existing capabilities. Finally, adversaries and rogue nations continue to develop their own missile capabilities, requiring the DoD to modernize its ballistic missile defense to meet current and emerging threats while balancing combatant commands' missile defense requirements. Investing in and modernizing the U.S. Space Force, the nuclear triad, and missile defense are critical challenges for the DoD to effectively counter the threats posed by adversaries and rogue nations.

The fifth challenge, "Enhancing Cyberspace Operations and Capabilities and Securing the DoD's Information Systems, Network, and Data," focuses on the critical role of cyberspace in supporting DoD business and military operations. The DoD continues to face sophisticated and evolving cyber attacks. DoD adversaries are constantly attempting to exploit cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target DoD critical infrastructures, manipulate information, and conduct cyber attacks. The DoD must continue to deploy and use cutting-edge technology to maintain its military and tactical advantage.

The seventh management challenge, "Ensuring Health and Safety of Military Personnel, Retirees, and Their Families," highlights one of the Secretary of Defense's top priorities. The DoD OIG merged two FY 2020 management challenges related to the welfare and well-being of service members and their families and military health care. The DoD is responsible for the mental and physical well-being of service members. To adequately treat, protect, and provide for its personnel, the DoD must carefully implement Military Health System reform and ensure that electronic health records are properly deployed and protected. In addition, behavioral health issues such as substance abuse and suicide prevention are key health and safety challenges for the DoD. Finally, environmental health and military housing have also been serious concerns for the DoD in protecting its personnel.

The eighth management challenge, "Strengthening and Securing the DoD Supply Chain and Defense Industrial Base," addresses the enduring challenges of sustaining weapons and systems. The supply chain is how the DoD provides the Military Services with the

supplies they need at the right place and time. The Defense Industrial Base provides the DoD with supplies ranging from meals ready-to-eat to tanks and missiles. The enduring challenges within the supply chain and Defense Industrial Base include limited sources of supply in the United States. A limited number of suppliers can lead to decreased readiness, sustainment, and security; reliance on foreign suppliers; delays in repairing equipment and systems; and potentially higher prices paid due to a lack of competition. However, changes in contract and acquisition policy and the use of alternative methods of manufacturing over the past few years have aimed to mitigate these enduring challenges. This challenge incorporates two FY 2020 management challenges, which focused on acquisition and contract management and on supply chain management and security.

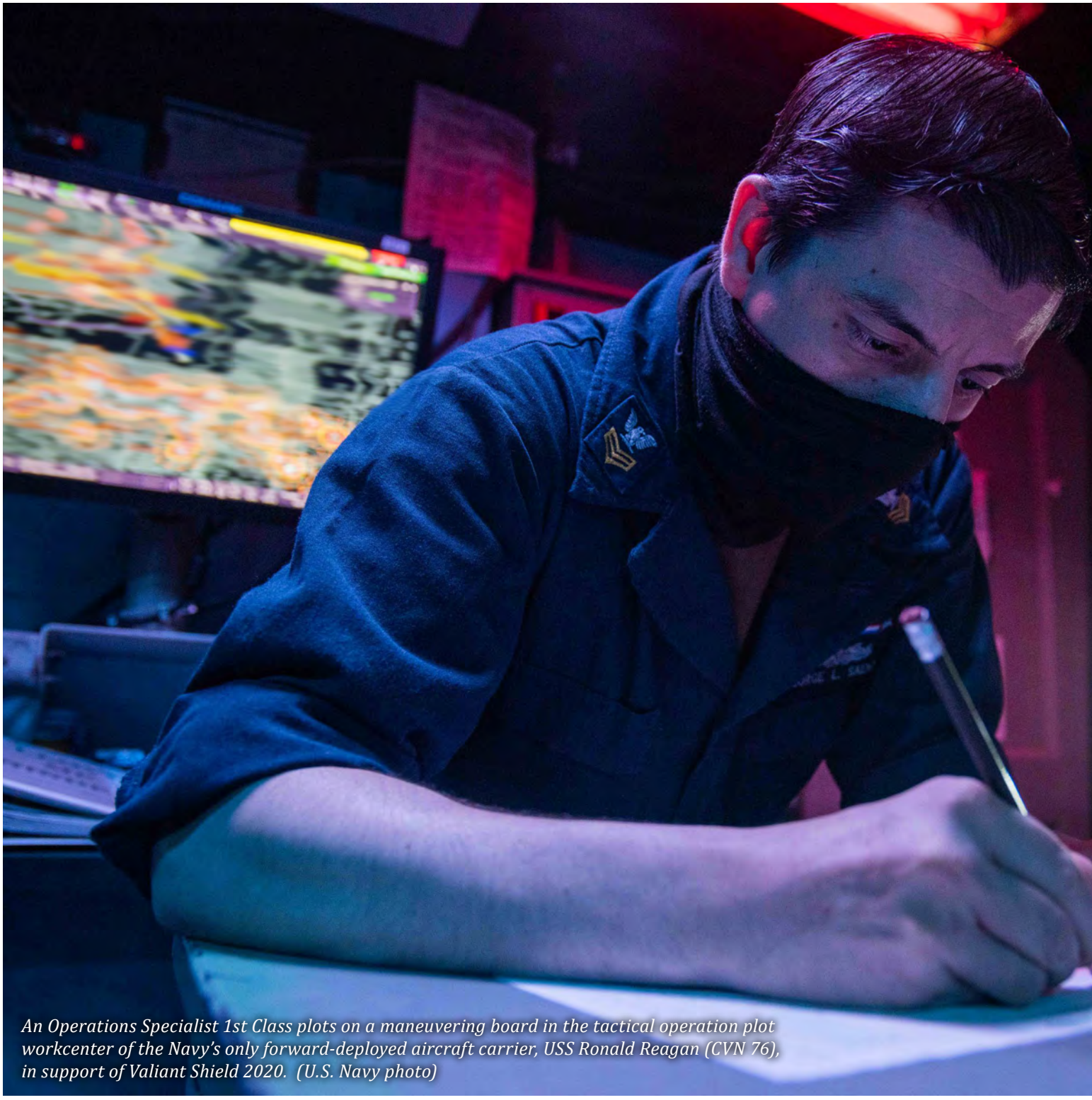
The ninth management challenge, "Improving Financial Management and Budgeting," addresses the longstanding financial management challenges that continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support reported financial statement balances. Additionally, the lack of reliable financial information impacts the DoD's operating, budgeting, and management decision making. One of the DoD's strategic objectives is to "improve the quality of budgetary and financial information that is most valuable in managing the DoD." Maintaining and using reliable, consistent, and timely enterprise data to support leadership decision making is of paramount importance.

U.S. Marines with 3rd Reconnaissance Battalion, 3rd Marine Division, patrol through water during a Marine Corps Combat Diving Supervisors Course on Camp Schwab, Okinawa, Japan, May 20, 2020. (U.S. Marine Corps photo)

The tenth management challenge, "Promoting Ethical Conduct and Decision Making," focuses on the critical issue of ethics within the DoD. The Secretary of Defense's August 2019 memo to all military personnel and DoD employees stated that the DoD enjoys the highest trust and confidence of the American people "because we live by core values grounded in duty and honor that influence how we think and act. The decisions we make every day reaffirm our commitment to ethical conduct—doing what is right, without hesitation." Ethics builds principled, self-disciplined teams; strengthens alliances and builds new ones; and is fundamental to business reforms. For example, the DoD has proactively issued a set of ethical principles for using artificial intelligence. However, in other areas, the DoD continues to address sexual assault in the military, sexual harassment in the DoD, and culture and accountability issues. The vigilance required to safeguard ethical conduct is rewarded by Americans' continuing trust and confidence in the DoD.

Finally, the DoD OIG recognizes the challenge of building a 21st century workforce. Although this issue is not a standalone challenge, several management challenges acknowledge the importance of recruiting, training, and retaining a modern workforce, specifically the management challenge regarding cyberspace, data, and information, and the challenge regarding financial management and budgeting. The issues of diversity and inclusion within the DoD workforce are critical to ensuring the DoD develops and retains the best workforce to meet the challenges laid out in this document and successfully executes its mission defending the United States.

The DoD considers these 10 challenges to be the most critical issues facing the DoD. The DoD OIG will use these challenges to provide the strategic guidance and inform its work in the next fiscal year, as outlined in the DoD OIG FY 2021 Oversight Plan.



An Operations Specialist 1st Class plots on a maneuvering board in the tactical operation plot workcenter of the Navy's only forward-deployed aircraft carrier, USS Ronald Reagan (CVN 76), in support of Valiant Shield 2020. (U.S. Navy photo)

Challenge 1. Maintaining the Advantage While Balancing Great Power Competition and Countering Global Terrorism

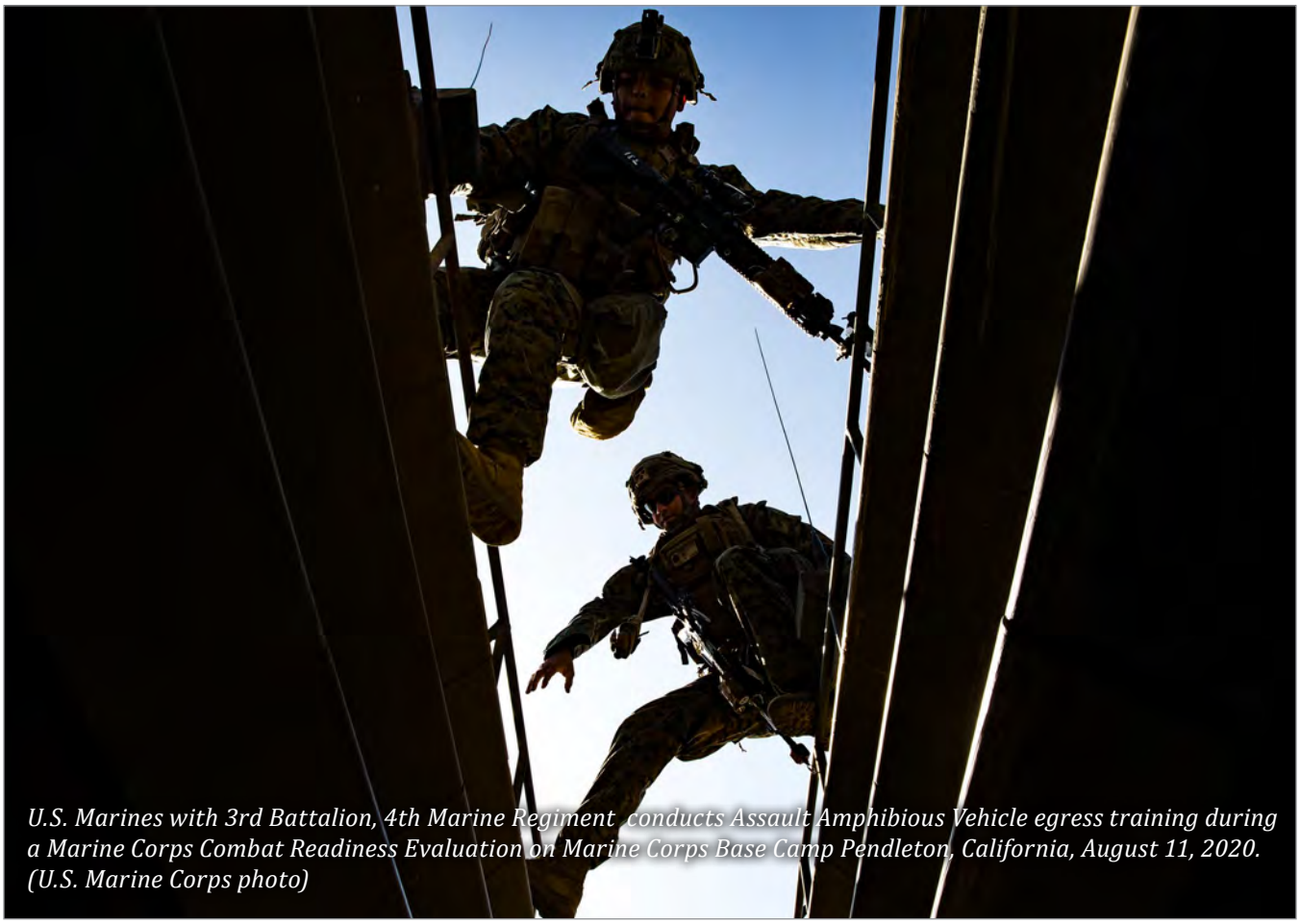
INTRODUCTION AND OVERVIEW

In the Chairman of the Joint Chiefs of Staff's Fiscal Year 2021 Defense Budget Posture testimony to the Senate Armed Services Committee on March 4, 2020, he said "our competitive advantage is eroded and no one should have any doubt about that. China and Russia are increasing their military capabilities to outmatch the United States and its allies in order to exert their global influence and China's objective is to do that by mid-century." The FY 2021 Defense Budget and the 2018 National Defense Strategy identify great power competition as the pre-eminent challenge facing the Nation's security. Revisionist nations, such as China and Russia, seek to assert their power and reshape the existing world order to their political, military, economic, and strategic benefit. Rogue regimes, such as Iran and North Korea, seek to destabilize their regions through efforts short of war, including pursuing nuclear weapons or supporting terrorism.

The rise of revisionist nations and continuing efforts by rogue regimes to challenge the United States' status as a global superpower forced a shift in U.S. defense strategy away from counterterrorism operations, which must still be conducted to deter and defeat violent extremist organizations. The challenge facing the DoD is maintaining the U.S. military's advantage while balancing great power competition and countering global terrorism through improved interagency collaboration and rebuilding military capabilities that have atrophied the past 20 years.

IMPROVING INTERAGENCY COLLABORATION TO ACHIEVE GREAT POWER COMPETITION OBJECTIVES

According to the National Defense Strategy, long-term strategic competition "requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military." The U.S. Government approach to great power competition involves developing unique strategies to counter revisionist powers, such as China and Russia, and rogue regimes, such as Iran and North Korea, that use corruption, predatory economic practices, propaganda, political



U.S. Marines with 3rd Battalion, 4th Marine Regiment conducts Assault Amphibious Vehicle egress training during a Marine Corps Combat Readiness Evaluation on Marine Corps Base Camp Pendleton, California, August 11, 2020. (U.S. Marine Corps photo)

subversion, proxies, and the threat or use of military force to affect their desired outcomes. These regimes seek to undermine U.S. relationships with foreign security partners by investing in the partners' infrastructure and providing military aid. The strategy further states that "a more lethal force, strong alliances and partnerships, American technological innovation, and a culture of performance will generate decisive and sustained U.S. military advantages."

The DoD has traditionally focused on objectives related to armed conflict, relying on its lethal military force and its power projection strategies and capabilities. In contrast, other U.S. agencies, such as the Department of State and the Department of the Treasury, specialize in enhancing national security through diplomacy and economic strategy. For instance, the Department of State is responsible for identifying foreign terrorist organizations, based on whether the organization poses a threat to the security of U.S. economic interests or foreign relations. The Department of the Treasury implements economic sanctions against those foreign threats by targeting financial support networks. The National Defense Strategy emphasizes that the "DoD must assist efforts of the Departments of State, Treasury, Justice, Energy, Homeland Security, Commerce, U.S. Agency for International Development, as well as the Intelligence Community, law enforcement, and others to identify and build partnerships to address areas of economic, technological, and informational vulnerabilities."

The Global Engagement Center, established in 2016 and led by the Department of State, is responsible for coordinating with the DoD and

other agencies to counter disinformation efforts and propaganda by near-peer competitors, adversaries, and terrorist organizations that aim to undermine U.S. national security interests. In August 2020 the State Department's Special Envoy for the Global Engagement Center stated that Russia and China both "leverage conspiracy websites and proxy channels to push disinformation and propaganda" with the goal of undermining democratic norms and institutions. In 2020, the DoD OIG identified a lack of interagency coordination while transitioning responsibilities for information support operations between the DoD and the State Department after the defeat of the caliphate of the Islamic State of Iraq and Syria (ISIS). This lack of coordination degraded the United States' ability to effectively influence attitudes, beliefs, and behaviors in Iraq.[1] Integrated efforts with other U.S. Government agencies enhance the DoD's ability to protect national security.[2]

Interagency collaboration is critical to the United States achieving its great power competition objectives. However, competing missions and priorities across U.S. Government agencies pose unique challenges for the DoD. Specifically, the DoD should ensure its strategies take into account other U.S. agencies' distinct authorities, cultures, strategies, priorities, and goals. DoD efforts should capitalize on or complement other agencies' efforts, even if those efforts do not easily align with the DoD's. Effective interagency collaboration will better enable the U.S. Government, as a whole, to successfully compete with, deter, and counter near-peer adversaries.

REBUILDING MILITARY CAPABILITIES

The National Security Strategy and National Defense Strategy state that the erosion of military capability has impacted all domains—air, land, sea, space, and cyberspace. Both documents call for building a more lethal and resilient force. The challenge for the DoD is to rebuild capabilities to effectively compete with near-peer rivals and other adversaries, while continuing to combat terrorists and insurgents. Rebuilding military capabilities includes modernizing capabilities, such as nuclear deterrence and missile defense; developing innovative operational concepts, such as cyber and space warfighting; and developing critical technologies, such as hypersonic weapons, artificial intelligence, and microelectronics.[3]

The DoD relies on sustained authorities and predictable appropriations to plan and resource programs and operations. Effectively planning for great power competition, including researching, developing, testing, evaluating, and procuring new capabilities, requires predictable budgets. However, the Congressional Budget Office report, "The 2020 Long-Term Budget Outlook," noted that deficits and the national debt are projected to grow over the next several decades, potentially causing "policymakers to feel restrained from implementing deficit-financed fiscal policy" to, among other things, strengthen national defense.[4] The DoD must be prepared to make

[1] Report No. DODIG-2020-065, "Evaluation of Combined Joint Task Force–Operation Inherent Resolve's Military Information Support Operations," February 27, 2020.

[2] Ibid.

[3] DoD, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," 2018; United States, "National Security Strategy of the United States of America," December 2017; and National Defense Strategy Commission, "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission," November 13, 2018.

[4] Congressional Budget Office, "The 2020 Long Term Budget Outlook," September 2020.

hard decisions regarding legacy systems and modernization investments to determine how it will compete against near-peer competitors, especially if budgets are flat or decline, and appropriations and authorizations are not predictable.

BUILDING A MORE LETHAL AND RESILIENT FORCE

For the United States to maintain its influence as a global leader, the DoD must restore, field, and sustain sufficient, capable, and lethal forces that are organized, manned, trained, and equipped to defeat a near-peer adversary across all domains. The growing threats of near-peer competitors and rogue regimes will only increase the demands on the U.S. military. The DoD must counter or deter near-peer power projection, asymmetric warfare tactics, and proliferation of advanced or nuclear technologies, while also defeating terrorist organizations and responding to events requiring humanitarian assistance.

The congressionally mandated, nonpartisan, independent Commission review of the 2018 National Defense Strategy, referred to as the National Defense Strategy Commission's Report, stated, "The United States is particularly at risk of being overwhelmed should its military be forced to fight on two or more fronts simultaneously."[5] To meet these multiple demands, the Commission said, "the United States needs a larger force than it has today if it is to meet the objectives of the [National Defense] strategy."[6]

The Commission identified several recommended improvements for the DoD to address eroding capabilities across all domains. For example, the Commission stated that the Air Force requires more aircraft and munitions for its mission set but more importantly needs more intelligence, surveillance, and reconnaissance platforms. The Commission also emphasized that the DoD must not get "hampered by debates over authorities and jurisdictional boundaries," which have lingered over multiple administrations. The DoD should also continue to invest in cyber defense, be able to quickly and effectively identify and recover from a cyber attack, and be fully integrated into the full spectrum of military operations.

The DoD requires a Joint Force with decisive advantages in any likely conflict, and must consider how emerging technologies can reshape the battlespace, enhance its existing capabilities, and reimagine future capabilities, doctrine, and tactics. Management Challenge 2, "Building and Sustaining the DoD's Technological Dominance," discusses the importance of emerging technology for both near-peer competitors and the United States. Management Challenge 4, "Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense," discusses the threats posted by China, Russia, Iran, and North Korea's investment in space-based capabilities; nuclear weapons; and short-, medium-, and long-range missiles.

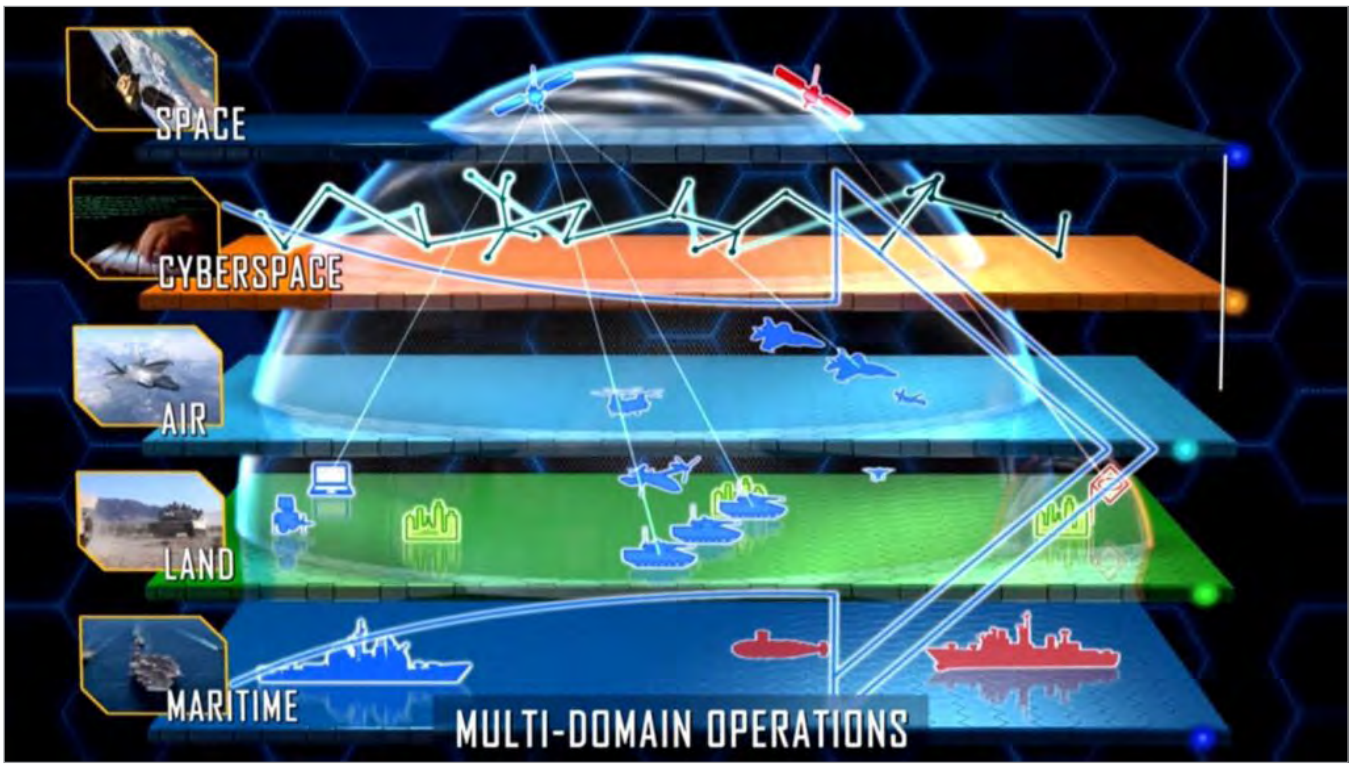
INNOVATIVE OPERATIONAL CONCEPTS TO SUPPORT GREAT POWER COMPETITION

In late 2019, the Secretary of Defense directed the Military Services and the Joint Staff to create a new Joint Warfighting Concept for All-Domain Operations by December 2020. The Vice Chairman of the Joint Chiefs of Staff stated, "[T]his Joint Warfighting Concept will describe

[5] National Defense Strategy Commission, "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission," November 13, 2018.

[6] Ibid.

Figure 1. Multi-Domain Operations, or All Domain Operations, envisions a new collaboration across land, sea, air, space, and cyberspace



Source: U.S. Army.

the capabilities and attributes necessary to operate in this future all-domain world." Before the Secretary's directive, several Military Services and DoD Components had proactively taken action to address their multi-domain operational concepts.

For example, the U.S. Army Training and Doctrine Command published a pamphlet in December 2018 that identifies multi-domain capabilities operating against a near-peer adversary. The U.S. Air Force's multi-domain operational concept, Multi-Domain Command and Control, published in 2018, focuses on air, space, and cyberspace. Additionally, the U.S. Air Force created the Multi-Domain Warfare Officer career path to fill command and control billets within the Air Force's operations centers. The Air Force graduated its inaugural Multi-Domain Warfare Officer class on October 9, 2019. Figure 1 illustrates multi-domain operations.

The oversight community is focused on assessing the DoD's efforts to rebuild military capabilities in these domains. Rebuilding military capabilities to address threats across all domains requires a well-coordinated approach and deconfliction of policies, budgets, equipment development, and training.

COUNTERING TERRORISM AND VIOLENT EXTREMISM

As the DoD reorients to address the challenges and threats of great power competition, it must retain sufficient capacity and capability to counter persistent threats from violent extremist organizations around the world. In the Middle East, ISIS is regrouping following the death of its leader, Abu Bakr al-Baghdadi, during a U.S. military operation in October 2019. Despite the defeat of the so-called ISIS "caliphate" in the region, ISIS remains a threat

A U.S. Marine Corps Lance Corporal ranges a target during exercise Summer Fury 20 in Yuma, Arizona, July 14, 2020. (U.S. Marine Corps photo)

in Iraq and Syria. Additionally, the Iranian government continues to support proxy terrorist organizations in countries across the region, including Bahrain, Yemen, Iraq, Lebanon, and Syria. In Afghanistan, two decades of U.S. military operations have weakened al-Qaeda and ISIS affiliates operating in the country, but there remains a potential for their resurgence following the planned withdrawal of U.S. troops.

Meanwhile, violent extremist organizations continue to expand their influence in Africa and Asia. In January 2020, al-Shabaab, an al-Qaeda affiliate, attacked Camp Simba, a Kenyan military base at Manda Bay, Kenya, killing three U.S. personnel. In West Africa, attacks by ISIS and al-Qaeda affiliates are steadily increasing. Small numbers of U.S. forces have deployed across the continent to conduct operations against these violent extremist organizations and train, advise, and assist host nation forces in counterterrorism operations. U.S. military advisers also support host nation forces in the Philippines, where an ISIS affiliate continues its campaign of violence against the Philippine government and citizens.

In recent years, the DoD has incrementally reduced the personnel and resources that it deployed for counterterrorism missions around the world. The overseas contingency operations budget—which accounts for a large portion of counterterrorism expenditures in Iraq, Syria, Afghanistan, the Philippines and on the African continent—has decreased each year from a peak of $187 billion in FY 2009 to $69 billion in the FY 2021 President's Budget. However, as the DoD shifts its attention and resources to great power competition, it will need to

retain the agility and capability to combat persistent and evolving threats from violent extremist organizations.

The shift to great power competition will require the DoD to continue to prioritize its counterterrorism objectives. In particular, the National Security Strategy emphasizes that the United States' allies and partners will continue to share responsibility in the fight against terrorism. In regions where the United States operates as part of a coalition or in coordination with international forces, the United States must highlight the vested interests in counterterrorism and lay the ground work to make joint contingency planning worthwhile. This may require the United States to identify gaps in capabilities and equipment, and encourage partners to commit more resources to counterterrorism missions.

In many countries, the United States provides training and equipment to host nation forces to help them build forces to counter violent extremism. These missions typically require years of commitment to achieve sustainable progress. In Afghanistan, U.S.- and coalition-trained Afghan special operations forces have improved their operational performance, but Afghan conventional forces continue to struggle with corruption and poor logistics, despite nearly two decades of international support. Similarly, the Iraqi Security Forces and Counterterrorism Service continue to demonstrate increased independence and operational maturity, yet they remain dependent on U.S. forces in certain functional areas, such as intelligence, surveillance, and reconnaissance; air support; and combined arms integration.

To create economy of effort, the DoD should identify intersections between the goals of great power competition and counterterrorism. For example, Russia and China sell weapons, finance debt, and build infrastructure in Africa, but they do not conduct counterterrorism operations or assist African governments in building institutional and operational capacity. Through U.S. security cooperation activities, the U.S. Government establishes itself as a "partner of choice" for African forces and can use that goodwill to influence other areas of policy.[7] Similarly, the U.S. Government provides counterterrorism equipment and training to the Armed Forces of the Philippines, in part to counter Chinese influence in the region. Continuing to put pressure on violent extremist organizations while refocusing on great power competition will challenge the DoD to leverage partners effectively, establish clear priorities, and maximize investments to rebuild military capacity.

CONCLUSION

The DoD plays a vital role in maintaining global peace by maintaining a clear U.S. military advantage, building and maintaining partnerships with other nations, and collaborating with other Federal agencies. The challenge for the DoD is implementing a strategy that will enable the United States to more effectively compete with China and Russia, while retaining sufficient capacity and capability to counter persistent and evolving threats from violent extremist organizations around the world.

[7] U.S. Senate, Committee on Armed Services, U.S. Africa Command Posture Hearing, January 30, 2020.

An MQ-9 Reaper, assigned to the 556th Test and Evaluation Squadron, armed with an AIM-9X missile sits on the flightline, September 3, 2020, at Creech Air Force Base, Nevada. (U.S. Air Force photo)

Challenge 2. Building and Sustaining the DoD's Technological Dominance

INTRODUCTION AND OVERVIEW

America's adversaries are developing sophisticated military and intelligence capabilities to target the United States and make it more difficult to defend against emerging technologies. From hypersonic weapons and microelectronics to artificial learning and 5G communications, these technologies will revolutionize warfare and enable the United States and its adversaries, especially great power competitors, to advance their interests. At the January 2020 Center for Strategic and International Studies forum, the Secretary of Defense stated, "[E]merging technologies will fundamentally transform the character of warfare in years to come." He noted, in particular, that China and Russia are "trying to use emerging technologies to alter the landscape of power and reshape the world in their favor." To build and sustain the DoD's technological dominance, the United States needs to solidify its competitive advantage by developing technologies such as hypersonic weapons, microelectronics, artificial intelligence, 5G communications, and biotechnologies, while also developing effective countermeasures to defeat adversaries' capabilities and protect against intellectual property theft and cybersecurity risks.

Whether identified as "systems confrontation" by the Russian military or "algorithmic warfare" by the Chinese People's Liberation Army, emerging technologies are rapidly evolving and transforming the conduct of war. The potential of emerging technologies, and the challenges for the DoD, may be reflected in the new ways of warfighting. Autonomous intelligent machines and applications can rapidly accelerate the speed of decision making and action, improve the DoD's understanding of the battlespace, and enable new missions not yet conceived. The DoD must be more agile and rapidly develop, secure, and deploy new and innovative technologies to secure the competitive advantage and counter similar technology.

HYPERSONICS

Hypersonics are weapons that travel faster than Mach 5 (or approximately 3,800 miles per hour or 1 mile in less than a second) and have the capability to maneuver during the entire flight. Unlike ballistic missiles of today, which fly fast and predictably, hypersonic missiles have the potential to fly faster and on an unpredictable path, making them more difficult to track and defend against. The abilities to travel at ultra-high velocity and maneuver during flight are the primary appeals of an offensive hypersonic missile capability because they allow the weapon to bypass modern layered missile defenses. These same offensive characteristics also create a significant defensive challenge.

Russia has been pursuing a hypersonic weapon program since the 1980s, and in the last 6 years, China successfully tested multiple hypersonic vehicles. According to the Congressional Research Service, open-source reporting indicates that both countries could begin fielding an operational—and potentially nuclear—capability in 2020.[8] At the August 2020 Space and Missile Defense Symposium, the Assistant Secretary of Defense for Strategy, Plans, and Capabilities stated, "China and Russia are developing and testing hypersonic missile technology with Russia recently deploying the world's first operational intercontinental-range hypersonic glide vehicle, the Avangard, and China not likely far behind." The United States is aiming to initially field an operational hypersonic weapon in 2023. At an August 2020 Space and Missile Defense event, the Director for Hypersonics, Directed Energy, Space and Rapid Acquisition, Office of the Assistant Secretary of the Army in Acquisition, Logistics and Technology said, "[W]e need to be aggressive in order to keep on pace and really be competitive with our near-peer competitors, namely Russia and China."

The Under Secretary of Defense for Research and Engineering acknowledged the threat of hypersonic weapons during his testimony to the Senate Armed Services Committee on April 18, 2018. He stated that the United States "does not have a system which can hold [China and Russia] at risk in a corresponding manner, and we don't have defenses against [their] systems."[9] He further stated, "It is among my very highest priorities to erase that disadvantage, creating our own systems to hold them at risk and to provide defense."

Congress and the DoD have prioritized the development and deployment of hypersonic weapons in recent years. The DoD is currently accelerating the development of prototype conventional (non-nuclear) hypersonic weapon programs in each of the Military Services as well as the Defense Advanced Research Project Agency.[10] For FY 2021, the DoD requested $3.2 billion for hypersonic weapons, a 23-percent increase over its FY 2020 request. The FY 2021 request includes a significant increase to funding hypersonic research by the Military Departments, especially the Army and Navy.

From a defensive perspective, traditional antimissile and other air defense measures are limited against hypersonic vehicles. In testimony before the Senate Armed Services Committee in April 2018, the Vice Chairman of the Joint Chiefs of Staff stated, "[W]e don't have any defense that could deny the employment of

[8] Congressional Research Service, "Hypersonic Weapons: Background and Issues for Congress," updated August 27, 2020.

[9] Statement of Mr. Michael Griffin, "Testimony Before the Senate Committee on Armed Services on New Technologies to Meet Emerging Threats," April 18, 2018.

[10] Ibid.

such a weapon against us."[11] Over the last few years, the DoD expanded the Missile Defense Agency's mission beyond regional and homeland defense to include serving as the executive agent for defense against hypersonic glide vehicles. The Government Accountability Office concluded in a 2020 report that the Missile Defense Agency faces technical challenges, and needs to ensure a sound acquisition approach, to develop hypersonic defenses.[12]

The DoD's challenges related to hypersonic weapons are discussed further in Management Challenge 4, "Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense," and Management Challenge 1, "Maintaining the Advantage While Balancing Great Power Competition and Countering Global Terrorism."

MICROELECTRONICS

Microelectronics support nearly all DoD activities, enabling capabilities such as the global positioning system, radar, command and control, and communications. Microelectronics refers to the design and manufacturing of extremely small electronic components, usually in the form of microchips and microcircuits. It affords increased performance and enhanced capability, usually through a smaller feature size, and is significant to weapon systems and key to the DoD's efforts to achieve and maintain technological superiority.

Ensuring secure access to leading-edge microelectronics, however, is a challenge. During the August 2020 Defense Advanced Research Projects Agency's Electronics Resurgence Initiative Summit, the Under Secretary for Defense for Acquisition and Sustainment stated that the DoD "can no longer clearly identify the pedigree" of its microelectronics. She stated that while the components are designed and circuit cards printed in the United States, the rest of the process—including fabricating, packaging, and testing—is largely done offshore. The Under Secretary continued that the result is that the DoD cannot ensure the security of the microelectronics, meaning that backdoors, malicious code, or data exfiltration commands could be embedded in the components. Ensuring a secure, resilient microelectronics supply chain requires the DoD to continue looking for a path to domestic sources for the important microelectronics that are used in defensive weapons now, and for microelectronics that will be needed in the future.

To address the security of the microelectronics supply chain, the DoD is moving toward a "zero trust" model to ensure the DoD develops and procures state-of-the-art microelectronics. The intent of the zero trust model is to allow the DoD to reduce and manage risks and vulnerabilities. This validation and verification process will be the key to a successful zero trust model. The DoD OIG in FY 2021 plans to evaluate whether the DoD has plans and procedures in place to manage and mitigate risks as it transitions from a trusted foundry model to a zero trust model for procuring microelectronics. Microelectronics represent a vital technology for the DoD, but one with potential risks the DoD must address.

ARTIFICIAL INTELLIGENCE

The DoD believes that investment in artificial intelligence (AI) and machine learning is critical to sustaining U.S. competitive military advantage. It established the Joint Artificial Intelligence Center in the Office of the

[11] Statement of Mr. Michael Griffin, "Testimony Before the Senate Committee on Armed Services on New Technologies to Meet Emerging Threats," April 18, 2018.

[12] Report No. GAO-20-432, "Missile Defense: Assessment of Testing Approach Needed as Delays and Changes Persist," July 23, 2020.

Chief Information Officer to accelerate and synchronize DoD-wide AI initiatives; released an AI Strategy; and, most recently, adopted a set of ethical principles for AI. The 2018 National Defense Strategy stated, "[T]he Department will invest broadly in military application of autonomy, AI, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages." In February 2020, the DoD Chief Information Officer stated that AI is the DoD's top technology modernization priority.

AI and machine learning have the potential to revolutionize how war is conducted by rapidly speeding up the collection and processing of data and information to facilitate analysis and decision making. AI and machine learning can impact a range of U.S. military functions, including intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and semiautonomous and autonomous vehicles. For example, in August 2020, an AI algorithm defeated a human fighter pilot in a virtual dogfight in the Defense Advanced Research Projects Agency's AlphaDogFight 2-day competition. The AI algorithm, aided by the system's ability to process data about its environment and begin to anticipate actions, defeated multiple AI teams prior to competing against the human fighter pilot. The competition was a significant step in understanding how AI and machine learning can be used in combat situations to potentially automate some tasks and allow humans to focus on performing strategic analysis and making decisions. The DoD's use of AI in logistics is discussed further in Management Challenge 8, "Strengthening and Securing the DoD Supply Chain and Defense Industrial Base."

AI integration efforts will affect a wide variety of DoD mission areas. The President's FY 2021 Budget requested funds for the Joint Artificial Intelligence Center's efforts across the Military Services. The Joint Artificial Intelligence Center established National Mission Initiatives focused on cross-Service or Component issues such as predictive maintenance and humanitarian assistance and disaster relief. The U.S. Army Futures Command is looking at AI in areas of human resources and talent management (human capital). The Defense Advanced Research Projects Agency's Explainable AI program aims to create a suite of machine learning techniques that, according to its website, could "enable human users to understand, appropriately trust, and effectively manage the emerging generation of artificially intelligent partners." AI has the potential to fundamentally change the conduct of war and presents opportunities and challenges for DoD senior leaders to reconsider institutional norms and effectively integrate it into programs and operations.

Despite their potential, AI and machine learning may also be vulnerable to manipulation by external threats, such as adversaries, near-peer competitors, and insider threats. More significantly, the DoD must maintain realistic expectations as well as address a cultural shift in developing and using AI to enhance weapon systems, analysis, and decision making. From a commercial perspective, private industry may be averse to working with the DoD and have concerns with its products being used for military purposes.

The Congressional Research Service has stated that commercial-off-the-shelf AI products cannot be easily used by the DoD and may require

modifications to be functional for the military.[13] The integration of AI with legacy platforms and information technology networks will continue to challenge AI development and deployment efforts. For example, the DoD's Project Maven, a program launched in 2017 to accelerate efforts to use AI and machine learning to process large volumes of data available to the DoD into actionable intelligence, was initially envisioned as a series of 90-day sprints, but experienced issues integrating the program with legacy systems. The program was also the source of significant tension between the DoD and Silicon Valley partners because contractor employees voiced concerns that they did not want to build warfare technology. This ethical concern is discussed in more detail in Management Challenge 10, "Promoting Ethical Conduct and Decision Making."

The DoD must maintain realistic expectations for emerging technology. A 2019 RAND report found that "it is important for [the] DoD to maintain realistic expectations for both performance and timelines," related to AI's development and use.[14] DoD senior leaders must consider how to develop and integrate AI capabilities while also positioning the military to counter advances made by competitors. More significantly, DoD senior leaders must thoroughly assess how AI and machine learning will alter the conduct of war.

5G NETWORK

The fifth generation (5G) of mobile technologies will improve upon the 4G network in data transfer speed and bandwidth, with significant implications for military operations.[15] The DoD recognizes that "those nations that master advanced communications technologies and ubiquitous [global] connectivity will have a long-term economic and military advantage."[16] Tomorrow's warfighters will use local and expeditionary 5G networks to move massive amounts of data and connect distant sensors and weapons into a dense, resilient battlefield network. 5G technologies have the capability to combine the DoD's current fragmented networks into a single network and provide improved situational awareness and enable timely, data-informed decisions. 5G also has the potential to strengthen existing missions like nuclear command, control, and communications, while also potentially improving the efficiency and speed of day-to-day tasks, such as logistics and maintenance. In FY 2021, the DoD OIG intends to conduct an evaluation to determine whether the DoD has policies and processes in place to protect 5G communications technologies from exploitation while it accelerates 5G development and deployment. The 5G capabilities do not come without risk.

According to the DoD 5G Strategy issued in May 2020, ensuring that the DoD can operate in a global 5G environment is challenging because U.S. adversaries and competitors seek to dominate the 5G market in key allied and partner nations. If the United States does not maintain technological dominance with 5G, then competitors or adversaries, such as China, could gain unauthorized network and data access via exploited components in the supply chain, malicious software, and insider threats. For example, in June 2020 the Federal

[13] Congressional Research Service, "Artificial Intelligence and National Security," updated August 26, 2020.

[14] RAND Corporation, "The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations," 2019.

[15] Congressional Research Service, "In Focus: National Security Implications of Fifth Generation (5G) Mobile Technologies," June 4, 2020.

[16] DoD, "5G Strategy," May 2, 2020.

An U.S. Air Force Technical Sergeant with the 321st Contingency Response Squadron security team, patrols with a Ghost Robotics Vision 60 prototype at a simulated austere base during the Advanced Battle Management System exercise on Nellis Air Force Base, Nevada, September 3, 2020. (U.S. Air Force photo)

Communications Commission (FCC) declared the Chinese companies Huawei and ZTE as threats to U.S. national security. The FCC Chairman stated that those companies are "risks to America's communications networks—and to our 5G future," due to their close ties to the Chinese Communist Party and China's military apparatus, which makes them broadly subject to Chinese law obligating them to cooperate with the country's intelligence services. These two companies are among the top five cellular technology producers in China, providing China the opportunity to become the global leader in supplying 5G infrastructure. U.S. dominance of the 5G market is critical to ensuring the DoD's ability to protect the networks from unauthorized access, malicious software, and other threats.

The DoD must also consider the potential vulnerabilities of sharing intelligence with allies and partners operating on Chinese-supplied 5G equipment. The Defense Innovation Board reported that China is likely to deploy the world's first 5G wide area network with more than 350,000 5G-operable base stations already deployed and more than 10 times as many as the United States.[17] A base station connects wireless devices with each other and can receive and transmit signals. If China becomes the global leader supplying 5G infrastructure to U.S. allies and partners, it poses a potential threat to the security of future DoD operations and networks. According to a Council on Foreign Relations article from August 2020,

[17] Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD," April 2019.

Huawei's 5G infrastructure could contain a backdoor, giving the Chinese government the ability to conduct cyber attacks.[18] Moving forward, the United States must not only build a sustainable 5G network, but also be able to ensure the security of that network across the DoD and commercial industries.

BIOTECHNOLOGY

Biotechnology is one of the DoD's modernization priority areas, with the potential to be a transformative national security technology. The National Defense Strategy identified biotechnology as one of "the very technologies that ensure we will be able to fight and win the wars of the future."[19] The DoD Office of the Chief Technical Officer defines biotechnology as a type of engineering that "utilizes or exploits living systems to produce a wide range of technologies and products" and can provide new capabilities across multiple domains, such as material and systems, military medicine, warfighter performance, and chemical-biological defense. For example, biotechnology can enable advanced bio-manufacturing that could provide the United States with domestic production of critical supply chain components, such as rare earth elements and pharmaceuticals.

The U.S. Government considers biotechnology a critical technology. The Committee on Foreign Investment in the United States, an interagency body chaired by a representative from the U.S. Department of the Treasury, can review certain transactions involving foreign investment in the United States and certain real estate transactions by foreign persons, to determine the effect of such transactions on the national security of the United States. Although the United States has dominated the biotechnology market, other nations are also investing in the research and development of biotechnologies. The U.S.-China Economic and Security Review Commission reported in 2019 that although Chinese investment in the U.S. biotechnology sector comprised only 2 percent of the overall Chinese investment (or $3.8 billion out of $175 billion) from 2000 to 2017, it is "one of the fastest growing sectors" of Chinese foreign direct investment, going from $21 million in 2012 to $531 million in 2014 and $1.5 billion in 2017.[20] Ensuring continued U.S. dominance in the biotechnology industry requires the DoD to continue prioritizing biotechnology research and development in modernization and funding decisions.

Biotechnology has potential for use in areas such as advanced materials, warfighter performance, military medicine, and chemical-biological defense. Adversaries are also investing in biotechnology and its applications, which presents risks for the DoD. These risks may also require DoD focus on chemical-biological defense to best support the warfighter and national security missions. Should the United States fail to fully invest in and develop biotechnology, it risks losing its position as the leader in this field.

According to the U.S.-China Economic and Security Review Commission's 2019 Annual Report to Congress, the Chinese government "designated biotechnology as a priority industry as a part of its 13th Five-Year Plan and the Made in China 2025 initiative."[21] China has

[18] Council on Foreign Relations, "Huawei: China's Controversial Tech Giant," August 6, 2020.

[19] DoD, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," 2018.

[20] Report prepared for U.S.-China Economic and Security Review Commission, "China's Biotechnology Development: The Role of U.S. and Other Foreign Engagement," February 14, 2019.

[21] U.S.-China Economic and Security Review Commission, "2019 Report to Congress."

signaled its willingness to use biotechnology and other emerging technologies against its opponents and adversaries without respect for international safety standards, conventions, or human rights. The DoD's 2020 Annual Report to Congress on Military and Security Developments Involving the People's Republic of China further highlighted China's commitment to investing in biotechnology, as well as other technologies, for the military to potentially improve the selection of soldiers, pilots, and special operators and their performance in combat and advance human-machine teaming.[22]

Given the serious biological threats posed by naturally occurring and human-modified pathogens, the President published the first ever U.S. National Biodefense Strategy in 2018.[23] According to the strategy, the DoD is prioritizing partnerships with the commercial sector to ensure biotechnology capability readiness and is focusing biotechnology modernization on three lines of effort: (1) critical capacity and infrastructure, (2) data as a strategic, operational resource, and (3) workforce development, to rapidly field biotechnology-enabled products for the warfighter.[24]

One of the three efforts is the establishment of biotechnology manufacturing innovation centers. Of the nine DoD manufacturing technology centers, two are focused on biotechnology. The first technology center, BioFabUSA in New Hampshire, opened in 2016 and focuses on regenerative manufacturing, or engineered tissues. The second technology center was announced in March 2020 by the Under Secretary of Defense for Research and Engineering. He stated that the new center will focus on "how to do in an industrial way what nature has done for us in so many areas of things that we harvest and mine and use." One particular area where this second center may dedicate attention is in the development of fuel through synthetic biology methods, or biofuel, which could help ensure the DoD has the requisite fuels to support national security missions and mitigate potential supply chain issues. Additionally, the Defense Advanced Research Projects Agency is also focusing heavily on biotechnology to combat bioterrorism, accelerate warfighter readiness, create biological means to protect U.S. troops, and meet adversary biological threats.

Biotechnology presents many challenges and opportunities for the DoD. Adversaries' development and use of biotechnology present significant risk to the United States. The DoD must continue to identify it as a modernization priority, given its potential to enhance warfighter performance, military medicine, chemical-biological, and material and systems.

PROTECTING U.S. TECHNOLOGICAL ADVANCES

In October 2018, the Secretary of Defense established the Protecting Critical Technology Task Force to align DoD efforts to protect critical technology and to better secure intellectual property and data. The Task Force Director stated in a November 2019 Defense News interview, "We are in a fight every day with our strategic competitors on our university campuses, in our businesses, in cyberspace. And the prize is military technological

[22] DoD, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," September 1, 2020.

[23] United States, "National Biodefense Strategy," 2018.

[24] Statement of Mr. Michael Griffin, Under Secretary of Defense for Research and Engineering, "Testimony Before the House Committee on Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities FY 2020 Science and Technology Posture Hearing," March 11, 2020.

advantage." In the last 20 years, adversaries and competitors have made significant technological investments and advances. The DoD must continue to invest, take risks, and challenge existing assumptions and notions of warfare to maintain the United States' technological dominance. Additionally, the DoD must build better relationships with industry—beyond the traditional defense industry companies—to take advantage of commercial advancements that could benefit the DoD.

Protecting emerging technologies for application in future capabilities is also critical to maintaining U.S. competitiveness in the global marketplace. For example, in 2019, the DoD OIG found that contracting offices inconsistently tracked which contractors maintained Controlled Unclassified Information on their networks and systems, putting the DoD at greater risk of that information being compromised by cyber attacks from malicious actors.[25] Malicious actors can exploit vulnerabilities on the networks and systems of DoD contractors and steal information related to some of the Nation's most valuable advanced defense technologies. In March 2020, the Under Secretary of Defense for Research and Engineering told the House Armed Services Subcommittee on Emerging Threats and Capabilities that the DoD "must be explicit about what we want to protect, from whom we want to protect it, and clever about how we do so, especially in regard to emerging technologies."[26] Protecting technological advances and superiority is critical to ensuring the DoD can deter and defeat competitors and effectively conduct its missions.

CONCLUSION

Emerging technologies affect all aspects of the DoD and are changing the conduct of war. U.S. competitors and adversaries are aggressively pursuing new technologies, such as hypersonic missiles, microelectronics, and AI, which could erode the United States' technological advantage and dominance. The DoD must build and sustain a future of technological dominance for the United States by focusing on the development, employment, defeat, and protection of emerging technologies.

[25] Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 25, 2019.

[26] Statement of Mr. Michael Griffin, Under Secretary of Defense for Research and Engineering, "Testimony Before the House Committee on Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities FY 2020 Science and Technology Posture Hearing," March 11, 2020.

Hawaii National Guard members assist with walk-up registration instructions for individuals in line to be tested for COVID-19, August 28, 2020, Honolulu, Hawaii. (U.S. Army National Guard photo)

Challenge 3. Strengthening Resiliency to Non-Traditional Threats

INTRODUCTION AND OVERVIEW

The recent increase in non-traditional threats, such as pandemics, changing climate, and extreme weather events, has presented the DoD with new challenges as it continues to defend and secure the Nation. In 2020, the coronavirus disease–2019 (COVID-19) pandemic has impacted DoD personnel and readiness. Secretary of Defense Mark Esper stated that the DoD's top three priorities during COVID-19 are protecting the DoD's people, maintaining military readiness, and supporting the whole-of-government interagency response. These priorities, while consistent with normal operational goals, can be complicated by a pandemic, which can negatively impact training, travel, and manning.

Changing climate and weather patterns, including extreme and damaging weather events, have adversely impacted military infrastructure and personnel readiness. Meanwhile, droughts, water scarcity, and other natural resource limitations offer opportunities for adversaries, competitors, and violent extremist organizations to exert their influence in pursuit of their goals. These challenges require the DoD to develop long-term plans to address these non-traditional threats without compromising its ability to defend the U.S. homeland and national security interests.

GLOBAL PANDEMICS

Global pandemics, such as the current COVID-19 pandemic, pose a threat to individuals, organizations, and nations. Aside from the health risks, pandemics can create or exacerbate political, social, and economic instabilities, while simultaneously offering opportunities for adversaries, competitors, and terrorists to advance their own objectives.

Global pandemics are caused by contagious viruses that can easily infect individuals and spread throughout a population in an efficient, persistent manner. Unique or novel pathogens, such as the virus that causes COVID-19, present challenges for the U.S. military, the Government, and the medical community because the pathogens can defy conventional diagnostic techniques and treatments, resulting in rapid spread through a community and nation.

Pandemics can negatively impact the combat readiness of DoD forces. For example, Army officials stated that as of July 20, 2020, approximately one in five soldiers (1,000 troops) in the active duty division were unavailable for training because they had either tested positive for COVID-19 or had been in contact with someone who might have had the disease. The Navy and the Marine Corps reported less throughput of basic trainees as a result of quarantines, social distancing, and limited housing. At a press briefing in July 2020, the Commanding General of the Marine Corps Training and Education Command said, "We know we will be short," referring to the number of recruits completing basic training. The Commander of Naval Service Training Command stated that while he thought the Command would be "on-track to meet the Navy's accession goal" for FY 2020, it had adjusted its accession processes and required new recruits to quarantine at an off-site location prior to arriving at boot camp.

Travel restrictions also impacted the ability of uniformed personnel and their families to change duty stations. For 60 days, from March 26 to May 26, 2020, permanent change of station (PCS) moves were prohibited. This restriction caused the PCS season, which usually runs from late spring to early fall, to be extended. Almost 30,000 service members and their families were waiting to PCS when the stop movement order was lifted on May 26, 2020. The cascading effect of not moving in a timely manner or transferring to new units while families remained at previous stations of duty imposes additional stresses on the service members and their families.

The DoD also had to scale back major military exercises because of the pandemic. For example, Defender-Europe 2020, planned for March 2020, would have been the third-largest military exercise in Europe since the end of the Cold War. The exercise tested the DoD's ability to deploy stateside forces to locations across Europe, including Poland, the Baltic states, some Nordic countries, and Germany. At the guidance of the Secretary of Defense and to implement COVID-19 prevention and mitigation efforts, Defender-Europe 2020 was modified in both scope and size, with the movement of U.S. troops stopped at the time and some linked exercises canceled. Without the benefit of in-person exercises and training, the DoD must identify alternative means to maintain readiness.

A pandemic can also stress supply chains and challenge the DoD's ability to maintain the readiness of its stockpiles, impacting the health, safety, and security of DoD personnel and their families. The Under Secretary of Defense for Acquisition and Sustainment stated during a July 2020 Brookings Institution event that the COVID-19 crisis exposed weaknesses in the DoD's supply chain. She said that the crisis increased awareness of fragilities throughout the U.S. supply chain and an overreliance on sources located in potentially adversarial countries like China. The DoD's challenges related to the supply chain and Defense Industrial Base are discussed further in Management Challenge 8, "Strengthening and Securing the DoD Supply Chain and Defense Industrial Base."

During the pandemic, the DoD was confronted with the task of maintaining unit and individual readiness, while simultaneously assisting the other Federal agencies with their responses to COVID-19 and other events. For example, more than 4,900 members of the Louisiana Army and Air National Guard's 11,000 total members supported both COVID-19 operations and Hurricane Laura response and recovery operations. As of September 2020, there were over 18,500 National Guard personnel performing medical and logistics duties in support of COVID-19 response. However, the added stresses of the pandemic, combined with longer

deployments and responses to natural disasters, may strain individual service members and the force. DoD leaders must ensure they are taking care of their people to prevent stresses that could lead to suicides or violent behavior without sacrificing readiness.

CHANGING CLIMATE AND EXTREME WEATHER EVENTS

Changing climate patterns and extreme weather events can have long-term impacts on personnel readiness and military infrastructure. The 2020 Atlantic hurricane season has been so active that the National Hurricane Center exhausted its list of storm names for only the second time since naming began in 1950. Droughts, water scarcity, and other natural resource limitations could exacerbate national security threats and the resiliency of governments as competition over scarce resources can lead to conflict. These challenges require the DoD to develop long-term strategies and plans to reduce its vulnerabilities and to address the threats to military infrastructure and personnel readiness.

Extreme weather events can directly jeopardize U.S. military installations and cause unplanned financial hardship on the DoD and local communities. For example, the financial impact of Hurricane Florence in 2018 caused $3.6 billion in damage at Marine Corps Base Camp Lejeune, North Carolina.[27] Flooding in 2019 caused over $1 billion in damage to infrastructure at Offutt Air Force Base, Nebraska. Recovering from these weather events and their impacts sometimes take years.

According to a 2020 RAND report, approximately 33 percent of the 78 Air Force sites within 2 kilometers of the coastline experience flooding, including six major Air Force installations and multiple critical communications and radar sites.[28] For example, the rock seawall protecting Alaska's Cape Lisburne Long Range Radar Station's northwest coastline has deteriorated over the past decade due to tidal and storm-driven wave action. As a result, the gravel airstrip protected by the seawall became unusable, forcing the Air Force to spend $46.8 million in 2018 to replace the 5,450-foot wall and protect the runway.

Some DoD Components have dedicated efforts to identify or mitigate the threats of climate change and extreme weather. In 2019, the Office of the Under Secretary of Defense for Acquisition and Sustainment published a report on the effects of climate change on the DoD.[29] The report stated that out of 79 installations reviewed in the continental United States, 53 are currently vulnerable to repeat flooding (see Table 1). Additionally, it stated that more than half of the 79 installations are at risk from drought and nearly half are vulnerable to wildfire.[30]

The U.S. Naval Academy in Annapolis, Maryland, participated in four studies between 2015 and 2019 to identify ways to mitigate flood water and high tide elevation threats. The Academy is expecting the sea level to rise between 0.6 and 3.6 feet by 2050, which would put much of the campus at risk of flooding. The Academy will be faced with the tough decision of either mitigating the risk by investing a significant amount of money to install pumps and barriers or by abandoning parts of the campus altogether. To assess the DoD's ability to address issues related to rising

[27] DoD, "Report on Effects of a Changing Climate to the Department of Defense," January 17, 2019.

[28] RAND Corporation, "Building Resilience Together: Military and Local Government Collaboration for Climate Adaptation," 2020.

[29] DoD, "Report on Effects of a Changing Climate to the Department of Defense," January 17, 2019.

[30] Ibid.

Table 1. Summary Table of Current and Potential Effects of Changing Climate on 79 Installations

		Recurrent Flooding		Drought		Desertification		Wildfires		Thawing Permafrost	
Service	**# Installations**	Current	Potential	Current	Potential	Current	Potential	Current	Potential	Current	Potential
Air Force	36	20	25	20	22	4	4	32	32	–	–
Army	21	15	17	5	5	2	2	4	4	1	1
Navy	18	16	16	18	18	–	–	–	7	–	–
DLA	2	2	2	–	2	–	–	–	–	–	–
DFAS	1	–	–	–	1	–	–	–	–	–	–
WHS	1	–	–	–	–	–	–	–	–	–	–
Totals	**79**	**53**	**60**	**43**	**48**	**6**	**6**	**36**	**43**	**1**	**1**

Legend:
DLA Defense Logistics Agency
DFAS Defense Finance and Accounting Service
WHS Washington Headquarters Services

Source: DoD, "Report on Effects of a Changing Climate to the Department of Defense," January 2019.

sea levels, the DoD OIG plans to conduct an audit in FY 2021 to determine whether Navy officials have appropriately planned for current and future environmental threats to naval shipyards, in accordance with Federal and DoD policies.

Other military installations are susceptible to droughts, desertification resulting from reduction in vegetation, wildfires, and thawing permafrost. For example, Army and Air Force installations in the western United States are vulnerable to desertification, which has limited training and testing due to the resulting increase in wildfires. The Canyon Wildfire at Vandenberg Air Force Base in California in September 2016 burned over 10,000 acres and threatened two space launch complexes. A year later, another wildfire burned 380 acres near Vandenberg, prompting the evacuation of personnel. Finally, the DoD has reported that thawing permafrost impacts bases in Alaska by decreasing "the structural stability of foundations, buildings, and transportation infrastructure," and that such thawing "requires costly mitigation responses that disrupt planning, operations, and budgets."[31] According to the report by the Office of the Under Secretary of Defense for Acquisition and Sustainment about the effects of climate change on the DoD, the "DoD must be able to adapt current and future operations to address the impacts of a variety of threats and conditions, including those from weather and natural events" and factor environmental impacts into its "mission planning and execution to build resilience."[32] Unfavorable weather conditions, such as extreme heat or cold, or dry and drought conditions that could limit training with explosives that may lead to wildfires, impact readiness by decreasing the number of available training days.[33]

[31] DoD, "Report on Effects of a Changing Climate to the Department of Defense," January 17, 2019.

[32] Ibid.

[33] RAND Corporation, "Building Resilience Together Military and Local Government Collaboration for Climate Adaptation," 2020.

Planning for future infrastructure and new DoD installations can take decades. The DoD should ensure that extreme weather and climate change are considered during facility design and investment decisions. The DoD's global property holdings are worth nearly $1.2 trillion. As the frequency of extreme weather events has increased, the DoD must consider the related risks and make wise investment decisions to mitigate the impacts of extreme weather on the DoD's mission.

U.S. military personnel, including the National Guard and Reserve Components, are routinely called upon to provide support to civil authorities for humanitarian assistance and disaster relief. For example, the DoD was integral to disaster response and relief efforts in Puerto Rico and the U.S. Virgin Islands in the wake of Hurricanes Maria, Irma, and Jose in 2017. The DoD deployed approximately 11,000 personnel after Hurricane Maria to focus on temporary power restoration; distribution of power generators; and the distribution of food, water, and fuel. In 2017, Hurricane Harvey caused $160 billion in damage and affected 13 million people in Texas and Louisiana; 13,000 National Guard, active duty service members, and DoD civilians deployed to provide direct and indirect humanitarian support. Additionally, every year the DoD provides support during wildfire season, but some seasons are more severe and require more DoD support than originally planned. During the 2018 and 2019 wildfire seasons, 2,300 National Guardsmen and 350 active duty military personnel assisted with wildfire fighting efforts.

Mitigating the impacts of changing climate patterns and extreme weather events on personnel readiness and military infrastructure is critical to building resiliency in the DoD force and on installations. The U.S. military has the unique capability to rapidly employ its personnel and logistics capabilities to respond to unexpected disasters and extreme weather events, which can potentially draw resources and personnel away from planned training, exercises, and other commitments.

GEOPOLITICAL IMPACTS OF A CHANGING CLIMATE AND EXTREME WEATHER EVENTS

Changing climate and the resulting extreme weather events can exacerbate geopolitical unrest. The stresses on natural resources undermine the capacity of nations to govern themselves, and increase the chance of conflicts. Forced migration, food insecurity, and the failure of governments to provide for basic needs make populations far more susceptible to extremism, political uprising, and wide-scale destabilization.

For example, a severe drought in Syria from 2009 to 2012 negatively impacted the agriculture industry, stoking unrest that led the nation into its ongoing civil war. Similarly, rising sea levels threaten to displace populations along the coasts of nations, such as Somalia and Yemen, that are hotspots for terrorism, which could lead to further instability.

For the last 70 years, India and Pakistan have had territorial disputes over Kashmir, including disputes over freshwater flowing from the melting glaciers in Kashmir. Increasing populations and threats of food insecurity complicate matters related to the freshwater supply provided by the melting ice. At least 330 million Indian citizens continue to be affected by drought and Pakistanis currently face alarming levels of malnutrition due to the same below-average monsoon rainfall and abnormally high temperatures seen in India. These changing environments present new security risks as nations compete for resources to protect their own interests and their people.

The geopolitical unrest that occurs as a result of the changing climate and extreme weather events can disrupt the DoD's ability to protect its national security interests around the world. To minimize this threat, the DoD must continue to integrate and update its risk mitigation strategies into its planning processes, which will help the DoD identify and address the most serious climate-related risks facing the global security environment.

THE EVOLVING ARCTIC SECURITY ENVIRONMENT

According to the DoD's 2019 Arctic Strategy report to Congress, the DoD recognizes the Arctic as part of the U.S. homeland, a "shared region," and a "potential corridor for strategic competition" between the Indo-Pacific region and Europe.[34] Due to a continuing loss of sea ice, the Arctic has started to shed its reputation as an inaccessible region. Including the United States, the following nations have territory above the Arctic Circle and are allied with the United States through the North Atlantic Treaty Organization—Canada, Denmark, Norway, and Iceland. However, the United States faces threats in the Arctic from both Russia, which possesses the most territory in the Arctic, and China, which identifies itself as a "Near-Arctic State" because it believes the region is tied to its future economic and strategic goals. As the Arctic region continues to open, the DoD may be called upon by its allies to provide security and stability to the region.

The Arctic has emerged as a strategic region due to its potential for natural resources and emerging sea lanes that are becoming navigable due to the loss of sea ice.[35] The United States has access to over 1 million square miles of territorial waters in the Arctic. From those waters, over $4.5 billion in seafood is fished each year by the Alaskan fishing industry. According to U.S. Government estimates, the entire Arctic region possesses over 90 billion barrels of undiscovered oil, 1,700 trillion cubic feet of natural gas, and $1 trillion of unmined rare earth minerals.[36] It is unclear who may claim ownership of resources that are under the seabed near the geographic North Pole, since most of that region is outside any nation's territorial waters and the 200-mile economic exclusion zone.

As the Arctic ice cap melts, increased national security risks arise from more shipping, military operations, and resource exploration in the Arctic. During the Cold War, the Arctic was seen as a back door to the United States for Soviet bombers and submarine-launched ballistic missiles. With the uptick in Russian submarine operations in the Arctic in recent years, this vulnerability still exists. Russia has steadily built up military facilities in its Arctic territory over the past decade. Most of these facilities are for defensive purposes, including radar stations, search and rescue facilities, and border posts. Russia has also reestablished Soviet-era air bases and air defense sites, and moved coastal missile systems into the region.[37] According to a 2017 Center for Strategic and International Studies report, Russia's military presence in the region enhances its defenses, secures the country's economic future, and creates a staging ground to project power.

The advent of new sea routes and resources has made the Arctic the newest theater in the era of great power competition. Even without the Northern Sea Route, Russia has a large economic interest in the Arctic due to oil, gas, and mineral extraction. According to the U.S. Air Force Arctic

[34] DoD, "Report to Congress: Department of Defense Arctic Strategy," June 6, 2019.

[35] Department of the Air Force, "Arctic Strategy," July 21, 2020.

[36] U.S. Coast Guard, "Arctic Strategy Outlook," April 2019; U.S. Geological Survey, "Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle," 2008.

[37] Department of the Air Force, "Arctic Strategy," July 21, 2020.

Strategy published in July 2020, close to 25 percent of Russia's gross domestic product is tied to the Arctic.[38] Besides having defensive assets in the region along the Northern Sea Route, Russia maintains a sizeable number of offensive assets in the region. The Russian Northern Fleet, based in Murmansk, is Russia's most important fleet. Most of Russia's nuclear attack submarines and ballistic missile submarines are part of the Northern Fleet because Murmansk offers the best access for the Russian navy to the Atlantic Ocean.

China considers itself a "Near-Arctic State," despite having no territorial claims in the region. China views the region as an important area for its economic and security interests and seeks to normalize and increase its presence through economic outreach, investments, and scientific activities. In 2018, China linked its Belt and Road initiative to the region, where it hopes to invest in ports and other infrastructure that would allow new shipping lanes to be more navigable. According to the U.S. Coast Guard's 2019 Arctic Strategy, China has taken interest in the region because of the potential for undiscovered oil and rare earth minerals, which are necessary for its continued economic growth.[39]

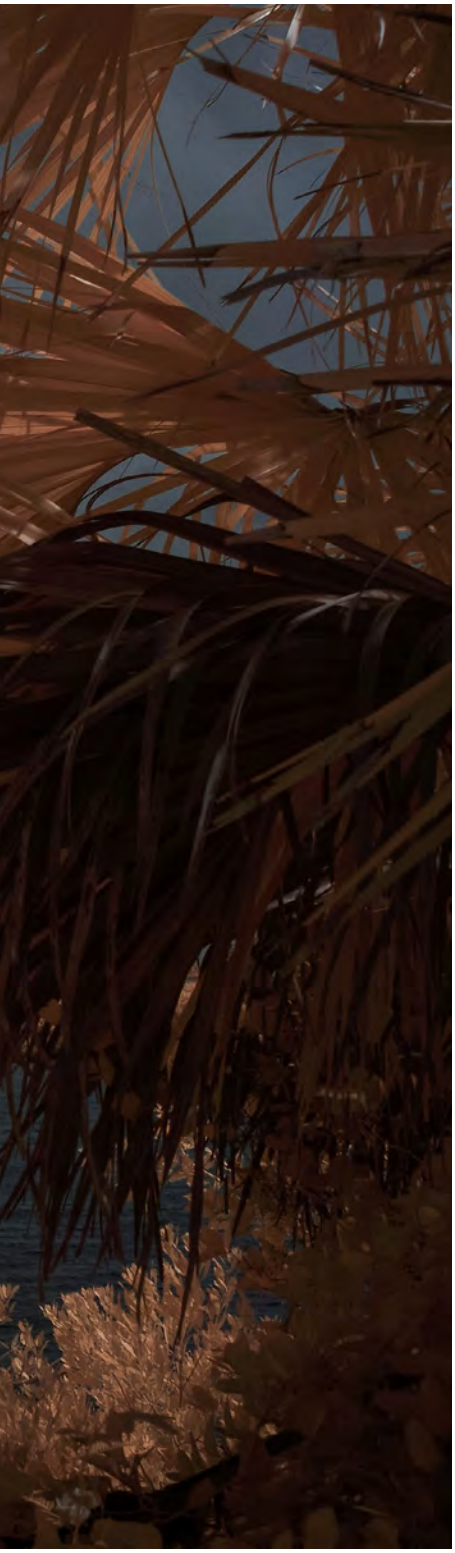
Furthermore, there is no overarching DoD command in charge of Arctic security. Instead, several commands have overlapping responsibilities. For example, U.S. Northern Command is responsible for the overall defense of Alaska, yet both 11th Air Force and U.S. Army Alaska, under Alaskan Command, a joint subordinate unified command of U.S. Northern Command, are also assigned to U.S. Indo-Pacific Command. The naval component of Alaskan Command is led by the Commander of the 17th Coast Guard District. U.S. European Command also has a role in the Arctic, as it has command of units that operate in the Norwegian and Barents Seas, and the northern Atlantic Ocean gap between Greenland, Iceland, and United Kingdom. This overlapping command responsibility could be a source of confusion and complicates DoD planning for contingencies. The DoD must address the overlapping command responsibilities to ensure seamless cooperation within the U.S. Government and with regional allies and partners. The Arctic security environment is an evolving challenge, but the DoD must evolve with it and continue to deter near-peer competitors and protect U.S. national security interests.

CONCLUSION

Whether the threat is a global pandemic, changing climate, extreme weather, or melting ice in the Arctic, non-traditional threats can impact U.S. national security. The DoD must consider the policy, resourcing, and operational impacts of non-traditional threats in current and future strategies, plans, and budgeting decisions. Global pandemics will change how the U.S. military operates as it maintains readiness while protecting its service members and their families from a contagious virus. Changing climate and extreme weather events will continue to affect military personnel, readiness, and training. The Arctic region, previously inaccessible, is becoming more accessible and opening the region to potential competition and militarization. If the DoD fails to address the impacts of non-traditional threats, then it will not effectively mitigate the increasing risks these threats present. These non-traditional threats will challenge the DoD's resiliency and ability to effectively defend the Nation.

[38] Department of the Air Force, "Arctic Strategy," July 21, 2020.
[39] U.S. Coast Guard, "Arctic Strategy Outlook," April 2019.

A SpaceX Falcon 9 rocket carrying two NASA astronauts launched from Launch Complexe 39A on NASA's SpaceX Demo-2 mission to the International Space Station, May 30, 2020, at NASA's Kennedy Space Center in Florida. (U.S. Marine Corps photo courtesy of NASA by Bill Ingalls)



Challenge 4. Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense

INTRODUCTION AND OVERVIEW

For decades, the DoD considered space an environment where space assets supported military operations in the air, on land, at sea, and in cyberspace. Today, space is a distinct competitive, contested, and congested warfighting domain. Missile defense and nuclear deterrence rely on the freedom of the U.S. military to operate in space, requiring an interconnected set of capabilities in this newly recognized warfighting domain. Adversaries are also investing substantially in their nuclear and missile capabilities, including developing advanced cruise missiles and hypersonic missiles that could pose a threat to U.S. forces and allies, as well as the U.S. homeland. These are urgent realities of the evolving missile threat environment that U.S. missile defense policy, strategy, and capabilities must address.

Investing in and modernizing the space force, the nuclear triad, and missile defense are critical for the DoD to effectively counter the threats posed by near-peer adversaries and rogue nations. Space-based capabilities—including missile warning; missile defense; kill assessment; attack assessment; and nuclear command, control, and communications—are a crucial component of U.S. deterrence. The establishment and transition of functions to the U.S. Space Force further complicates the modernization and sustainment of space-based capabilities. The nuclear triad—ballistic missile submarines, land-based intercontinental ballistic missiles, and bomber aircraft—and the nuclear command, control, and communications systems are rapidly approaching the end of their planned service lives. During a January 2020 nuclear modernization panel, the Deputy Commander of U.S. Strategic Command (USSTRATCOM) acknowledged the challenge to the nuclear triad when he observed that the DoD "currently finds itself trying to replace several components of its aging nuclear deterrent at the same time...[we] haven't staggered them...[and that] has presented a challenge to the military." The Ballistic Missile Defense System includes land-, sea-, and space-based elements to track, target, and destroy offensive ballistic missiles. Modernizing and expanding missile defense system capacity is critical to defending the U.S. homeland and allies. The proliferation of offensive ballistic and

cruise missiles, and emerging hypersonic weapon technologies, from adversaries presents challenges for the U.S. military's ballistic missile defense capabilities.

THREATS BY ADVERSARIES AND COMPETITORS

Adversaries and rogue nations are investing in space, nuclear weapons, and missile capabilities. The Secretary of Defense stated in June 2020, "We desire a secure, stable and accessible space domain that underpins our Nation's security, prosperity, and scientific achievement. However, our adversaries have made space a warfighting domain and we have to implement enterprise-wide changes for this new strategic environment." Near-peer adversaries and rogue nations present significant security challenges for the U.S. military to assuring space dominance, nuclear deterrence, and missile defense.

China. The People's Republic of China has devoted significant economic and political support to its space program, nuclear forces, and missile programs over the past decade. According to the Defense Intelligence Agency's (DIA) 2019 Space Assessment, China sees space as a vital theater for national pride, economic prosperity, and national security. President Xi Jinping is committed to building China into a "space power in all respects," to achieve "China's Dream" of a powerful nation.[40] China is developing a very capable counter-space system that consists of kinetic, electromagnetic, and direct energy systems in order to deny its enemies access and freedom of operation in space. Writings by the People's Liberation Army emphasize "destroying, damaging, and interfering with the enemy's reconnaissance… and communications satellites," which suggests that, in combat, China would quickly target an adversary's satellites.[41]

Regarding nuclear weapons, China's nuclear weapons policy "prioritizes the maintenance of a nuclear force able to survive a first strike and respond with sufficient strength to inflict unacceptable damage on an enemy," according to the DoD's 2020 Annual Report to Congress on Military and Security Developments Involving the People's Republic of China.[42] At the Chinese Communist Party's 2017 Congress, President Xi directed the People's Liberation Army to be "fully transformed into a first tier force" by 2050.[43] China aims to achieve this goal by having a true "triad" nuclear force that will consist of road-mobile and silo-based intercontinental ballistic missiles, submarine-launched ballistic missiles on new and advanced ballistic missile submarines, and a strategic bomber that is currently under development. The DoD's 2020 Annual Report also stated, "Over the next decade, China's nuclear warhead stockpile—currently estimated to be in the low 200s—is projected to at least double in size as China expands and modernizes its nuclear forces."[44]

Finally, China continues to develop advanced cruise missiles and hypersonic missile capabilities that can travel at exceptional speeds with unpredictable flight paths that challenge existing defensive systems. According to the DoD's 2020 Annual Report, in 2018 China

[40] Defense Intelligence Agency, "Challenges to Security in Space," January 2019.

[41] Defense Intelligence Agency, "China Military Power Report," 2019.

[42] DoD, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," September 1, 2020.

[43] DoD, "Nuclear Posture Review," 2018.

[44] DoD, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," September 1, 2020.

successfully tested what it publicly described as a hypersonic vehicle. A year later at the People's Republic of China 70th anniversary parade, the People's Liberation Army paraded for the first time its new supersonic cruise missile and hypersonic glide vehicle. Continued advances in space, nuclear forces, and missile capabilities by China pose serious threats to U.S. military dominance and require the DoD to assess its policy, strategy, capabilities, and investments in these areas.[45]

Russia. According to the DIA's 2017 Russia Military Power report, the Russian Federation under President Vladimir Putin seeks to reassert its role as a "great power on the global stage" by building a military capable of projecting power, defending its interests, and deterring the United States and members of the North Atlantic Treaty Organization (NATO).[46] Russia views space as a decisive battleground in future conflicts. Russia's 2014 update to military doctrine identified militarized space as an "extreme military danger" and viewed U.S. space systems as a threat to Russia because the systems enhance U.S. global strike capabilities.[47] The U.S. Space Force Chief of Space Operations described Russia's military actions in space by stating, "[T]hey're real, they're serious, and they're concerning." Russia also recognizes U.S. reliance on space for military operations, and believes that interdicting operations and access to space will disrupt U.S. military operations. Russia has developed and fielded ground, air, and space-based platforms over the past decade that can disrupt or destroy U.S. space assets.

In 2020, Russia demonstrated the ability to intercept and operate satellites in close proximity to U.S. satellites. In January and February 2020, two Russian satellites came within 100 miles of a National Reconnaissance Office satellite and have remained in close proximity ever since. This proximity could provide Russia the opportunity to photograph classified satellite designs or damage a satellite by colliding with it. Currently, the only effective defense against interceptors is to maneuver a satellite into a new orbit, which requires finite maneuvering fuel that reduces the on-orbit life of a satellite. In April 2020, Russia tested a ground-launched missile capable of destroying satellites in low-earth orbit, which puts most U.S. imagery reconnaissance satellites at risk. The U.S. Space Force Chief of Space Operations stated that the tests are "further proof of Russia's hypocritical advocacy of outer space arms control proposals designed to restrict the capabilities of the United States while clearly having no intention of halting their counter-space weapons programs." In July 2020, Russia conducted a possible test of a kinetic antisatellite system. Russia may have also developed the capability to intercept satellites in geostationary orbit, where most communication and navigation satellites are located.

The 2018 Nuclear Posture Review states that Russia has adopted an "escalate to de-escalate" nuclear doctrine. This doctrine means that if Russia is faced with the likelihood of defeat in a military conflict with NATO forces, Russia may threaten to use nuclear weapons to force NATO to withdraw its forces from the battlefield.[48] The Nuclear Posture Review also notes that while Russia has reduced its strategic nuclear weapon stockpile, it retains a large number

45 DoD, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," September 1, 2020.

46 Defense Intelligence Agency, "Russia Military Power Report," 2017.

47 Ibid.

48 Congressional Research Service, "Russia's Nuclear Weapons: Doctrine, Forces, and Modernization," July 20, 2020.

of non-strategic nuclear weapons. Russia is modernizing both its strategic and non-strategic nuclear weapons to expand the size of its nuclear arsenal, as well as increase its warhead delivery capacity. Russia's non-strategic weapons include theater-range and tactical-range nuclear weapons that are not subject to New Strategic Arms Reduction Treaty limitations. The Nuclear Posture Review also states that Russia believes these weapons "may provide useful options for escalation advantage."

Russia continues developing ballistic missiles that can carry multiple independently targetable warheads, hypersonic weapons, autonomous underwater weapons, and nuclear-powered cruise missiles with unlimited flight time. Although Russia faces challenges funding its modernization efforts due to low oil prices and economic problems, Russia will continue modernizing its space and missile capabilities, along with its nuclear weapon stockpile. This compels the DoD to consider its own strategies and investments to counter Russian aggression and protect U.S. national security interests.

Iran. The Islamic Republic of Iran is focused on developing its space program and missile capabilities, while continuing to harbor nuclear weapons ambitions. Iran's space program supports military and civilian goals, including boosting national prestige and advancing economic and scientific interests.[49] According to the DIA Challenges to Security in Space report, Iran's orbital launch capabilities are very limited in their ability to launch microsatellites into low-earth orbit.[50] As a result, the primary goal of its space program may be to use orbital launch vehicles as a test bed for intercontinental ballistic missile technology.

The DIA does not believe Iran possesses complex counter-space systems, due to their cost and technical complexity. Instead, it believes that Iran focuses on disruptive counter-space technology, such as cyber attacks and jamming. According to the DIA, Iran recognizes the strategic value of denying the United States' space-based capabilities. Iran has publicly acknowledged that it possesses the ability to jam GPS and commercial and military communication satellites.[51] The DIA also reported that the Iranian government has satellite communications and GPS jamming capabilities, and is believed to be a significant proliferator of GPS jammers.[52]

According to the Nuclear Posture Review, despite ongoing sanctions, Iran retains the technological capability and capacity necessary to rapidly develop a nuclear weapon.[53] Iran's development of increasingly long-range ballistic missile capabilities, along with its aggressive strategy and activities to destabilize regional governments, raise questions about its long-term commitment to forgoing nuclear weapons capability.[54] According to a 2018 DIA threat assessment, Iran has the region's largest ballistic missile arsenal, with close-, short-, and medium-range systems that can strike targets throughout the Middle East. The Iranian government continues to pursue long-range, precision land-attack cruise missiles,

[49] Defense Intelligence Agency, "Challenges to Security in Space," January 2019.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] DoD, "Nuclear Posture Review," 2018.

[54] Ibid.

demonstrating that it remains a threat to U.S. national security interests and regional allies and partners.[55]

Iran maintains a significant arsenal of short-, medium-, and long-range ballistic missiles that can target most U.S. bases in the Middle East. Iran demonstrated some of its capability in January 2020 when it launched 17 ballistic missiles at U.S. bases in Iraq in retaliation for the killing of General Qasem Soleimani, the Islamic Revolutionary Guard Corps' Quds Force Commander, in a U.S. drone strike. In August 2020, Iran unveiled two new missiles: a medium-range solid fuel ballistic missile and a ship-launched cruise missile. Iran remains a regional threat and its focus on space programs and nuclear weapons are threats the DoD must consider as it develops its own capabilities.

North Korea. The Democratic People's Republic of Korea presents a destabilizing force and threat to U.S. national security interests in the Asia-Pacific region. North Korea's space program, like Iran's, has long been considered a disguise for intercontinental ballistic missile technology testing. According to the 2018 Nuclear Posture Review, North Korea is pursuing nuclear weapons and missile capabilities in violation of United Nations Security Council resolutions.[56] Despite its rudimentary counter-space capabilities, the DIA has reported that North Korea has demonstrated non-kinetic counter-space capabilities, including GPS and satellite communication jamming.[57]

North Korea refuses to give up its nuclear weapons program, and continues to produce plutonium and highly enriched uranium to threaten and deter the United States and its allies in the Asia-Pacific region.[58] According to the DIA, the regime continues testing ballistic missiles—short, medium, intermediate, and intercontinental.[59] Some of these ballistic missiles have an estimated range capable of hitting Guam, Hawaii, and Alaska, as well as the U.S. mainland. North Korea also continues its nuclear detonation testing with ever-increasing seismic signatures, including one test in 2017 that it announced as a "hydrogen bomb."[60] North Korea has not carried out a test of a long-range missile since 2017, but did carry out several tests of short-range missiles and one test of a submarine-launched missile in 2019. According to a September 2020 State Department advisory, North Korea persists in trying to acquire missile technology from the private sector, in violation of U.S. and United Nations sanctions. North Korea's pursuit of nuclear weapons and missile capabilities will continue to present regional threats to the United States and its allies and partners.

SPACE DOMINANCE

In the 2020 Space Strategy, the DoD defined space as a "source of and conduit for national power, prosperity, and prestige," and vital to U.S. national security and economic prosperity. The DoD relies on space-based systems for communication, weather, intelligence, navigation, and a variety of other critical functions. These

55 Defense Intelligence Agency, "Worldwide Threat Assessment," March 6, 2018.

56 DoD, "Nuclear Posture Review," 2018.

57 Defense Intelligence Agency, "Challenges to Security in Space," January 2019.

58 DoD, "Nuclear Posture Review," 2018.

59 DoD, "Military and Security Developments Involving the Democratic People's Republic of Korea: Report to Congress," 2017.

60 Ibid.

systems allow the U.S. military to conduct operations across the world in support of its national security objectives.

SPACE FORCE

The creation of the U.S. Space Force was an important step toward assuring space dominance. The DoD faces the multiple challenges of resourcing the new Component, establishing policies to clarify roles and responsibilities, and streamlining operations—all while sustaining ongoing operations. The National Defense Authorization Act (NDAA) for FY 2020 abolished the Air Force Space Command and reassigned its 16,000 personnel to the Space Force. The FY 2020 NDAA also gave the Secretary of the Air Force the authority to transfer Air Force personnel to the Space Force. Although units from other branches must be transferred by FY 2023, the Space Force is initially focused on transferring over 6,000 Air Force personnel by the middle of FY 2021. The Space Force and the DoD still need to identify which units from the Army and Navy will transfer to the Space Force, and the two Military Services have expressed concerns about transferring missions and resources. The Secretary of the Air Force must ensure the Space Force has the necessary resources and authorities and must balance the new Military Service's budgetary priorities with Air Force resource priorities and requirements to effectively address national security threats.

Another significant challenge for the DoD is consolidating all space acquisitions into one seamless, proactive, and consolidated effort. Current plans call for most DoD Components involved in space acquisitions to fall under Space Force control, which presents a consolidation challenge because the acquisition programs are currently decentralized, fragmented, and uncoordinated across the DoD and other Government agencies.[61] Established in March 2019, the Space Development Agency is responsible for developing and fielding new military space capabilities necessary to ensure U.S. technological and military advantage in space. Although the Space Development Agency reports to the Office of the Under Secretary of Defense for Research and Engineering, Congress has directed the Space Development Agency to be transferred to the Space Force by October 2022. Consolidating all space acquisition programs, including Army and Navy space acquisition organizations and the Air Force's Space Rapid Capability Office, could enable one organization to oversee cost, schedule, and performance of acquisitions and better coordinate with industry partners to speed up the process of developing and fielding military space systems. The DoD OIG intends to evaluate the DoD's progress in developing and implementing a strategy for an integrated test program to validate the survivability of space-based systems in a contested space environment. Historically, most testing has focused on natural threats and launch integration, but testing must now be done against man-made threats, as other nations have unveiled more sophisticated counter-space systems.

SPACE LAUNCH

One of the most important acquisition decisions made by the Space Force's Space and Missile Systems Center was regarding the future of National Security Space Launches. In August 2020, the Air Force selected United Launch Alliance and Space Exploration

[61] Report No. GAO-17-619T, Testimony Before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. Senate, "Space Acquisitions: DoD Continues to Face Challenges of Delayed Delivery of Critical Space Capabilities and Fragmented Leadership," May 17, 2017; RAND Corporation, "Acquisition of Space Systems, Volume 7: Past Problems and Future Challenges," 2015.

Technologies Corporation (SpaceX) to launch national security satellites for the U.S. military and intelligence agencies. These contract awards mark an important transition of the national security launch program to take advantage of commercial innovation and private investments in launch vehicles. The awards also transitioned the DoD away from reliance on Russian RD-180 rocket engines. The Assistant Secretary of the Air Force for Acquisition, Technology and Logistics stated, "Maintaining a competitive launch market, servicing both Government and commercial customers, is how we encourage continued innovation on assured access to space."

According to the 2020 RAND Report, "Assessing the Impact of U.S. Air Force National Security Space Launch Acquisition Decisions," the commercial need for U.S. heavy-lift launch vehicles is expected to grow only moderately over the next decade.[62] As a result, the U.S. may not need multiple providers for heavy-lift launch vehicles. Government orders are the majority of the business for U.S. companies and some U.S. companies may permanently exit the heavy-lift launch vehicle market if they cannot secure Government orders. If the number of U.S. companies that provide these vehicles is too limited, the production and developmental costs could increase for future launch vehicles as a result of limited competition. The DoD OIG intends to evaluate the extent to which the DoD maintained launch facilities to meet anticipated launch requirements and the DoD's ability to increase the number of launches. Ensuring access to space requires the United States to have a steady supply of launch vehicles.

[62] RAND Corporation, "Assessing the Impact of U.S. Air Force National Security Space Launch Acquisition Decisions: An Independent Analysis of the Global Heavy Lift Launch Market," 2020.

NUCLEAR DETERRENCE

The strategic nuclear triad consists of submarines armed with ballistic missiles; land-based intercontinental ballistic missiles; and strategic bombers carrying gravity bombs and air-launched cruise missiles. The DoD is facing challenges regarding the obsolescence of most triad components and is planning to spend almost half a trillion dollars on modernization through 2030.

NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS

According to the 2018 Nuclear Posture Review, while the U.S. nuclear command, control, and communications system was once state-of-the-art, the system today is now subject to challenges from both aging system components and evolving 21st century threats. During peacetime and crisis, the nuclear command, control, and communications system performs five crucial functions: detection, warning, and attack characterization; adaptive nuclear planning; decision making conferencing; receiving presidential orders; and enabling the management and direction of forces. Nuclear command, control, and communications capabilities provide the President with the means to authorize the use of nuclear weapons in a crisis. Nuclear command, control, and communications capabilities are fielded through a large and complex system of land-based, air-based, and space-based components to ensure connectivity between the President and nuclear forces. Responsibilities for managing the system are distributed among many DoD Components, including the Military Departments, combatant commands, defense agencies, the Joint Staff, and the Office of the Secretary of Defense. The DoD OIG intends to evaluate the resiliency and vulnerabilities of the nuclear command, control, and communications

system to electronic and directed energy antisatellite systems. As other nations are testing and fielding an increasing number of electronic and directed energy antisatellite systems, it is critical that the nuclear command, control, and communications system is hardened against these attacks.

Growing threats in space and cyberspace, adversaries' nuclear escalation strategies, and the broad diffusion within the DoD of authority and responsibility for governance present challenges for an integrated nuclear command, control, and communications system. In 2018, the Secretary of Defense designated the USSTRATCOM Commander as the lead for the nuclear command, control, and communications enterprise with increased responsibilities for operations, requirements, and systems engineering and integration. The Secretary of Defense also approved the designation of the Under Secretary of Defense for Acquisition and Sustainment as the capability portfolio manager for nuclear command, control, and communications with increased responsibilities for resources and acquisition. These designations should more clearly define the authorities and responsibilities within the DoD. Modernizing the system is critical to ensuring nuclear command, control, and communications are not compromised if the space domain is denied.

BALLISTIC MISSILE SUBMARINES

Submarines armed with ballistic missiles perform a specialized mission of strategic nuclear deterrence and power projection. They carry long-range ballistic missiles, armed with multiple nuclear warheads, and remain hidden at sea to deter a nuclear attack on the United States. Their presence and capabilities demonstrate to other countries that the United States has a survivable, second-strike capability in case of a nuclear attack.

The Navy must balance the procurement and deployment of its new class of ballistic missile submarines while also maintaining the existing, aging submarines and ensuring no gap in nuclear deterrence. The Navy currently has 14 *Ohio*-class ballistic missile submarines that are scheduled to be replaced by 12 new *Columbia*-class ballistic missile submarines to modernize the Nation's seaborne leg of the nuclear triad. First built and launched in the 1980s, the *Ohio*-class originally had a 30-year service life, but the first *Ohio*-class submarine will reach the end of its extended 42-year service life in 2027, with the remaining reaching the end of their service life each year through 2040.

The *Columbia*-class is the Navy's top acquisition priority. The Navy plans to buy the first *Columbia*-class boat in 2021. However, the boat will not be delivered until 2028, assuming there are no cost overruns or schedule delays. According to the USSTRATCOM Commander, the new boat must undergo substantial testing and sea trials with the goal of being ready for its first deterrent patrol in 2031.[63] The Navy intends to procure the remaining *Columbia*-class submarines from 2024 through 2035, which means the boats will be delivered from 2031 through 2042. Under this projected schedule and the planned retirement dates for *Ohio*-class boats, the Navy expects that the nuclear ballistic submarine force would decline between FY 2027 and FY 2037, before increasing in FY 2041 and FY 2042. The Navy reported that the reduction to 10 or 11 boats between FY 2030 and FY 2041 is acceptable

[63] U.S. Strategic Command Posture Hearing, February 13, 2020.

for meeting strategic nuclear deterrence requirements because it is assuming that all 10 or 11 of the *Columbia*-class submarines in service will be operational during this period.[64] Although the Navy acknowledges the risk in having the nuclear ballistic submarine force drop, it provides little margin for absorbing an unforeseen event that delays the construction, testing, or maintenance of a nuclear ballistic submarine.

The Navy could face *Columbia*-class procurement issues associated with cost projections and price increases that often occur with new programs, as well as technology challenges. The challenge for the Navy is that it must continue to maintain the *Ohio*-class submarine fleet in service until the *Columbia*-class submarines are put to sea. The risks associated with fielding new programs on time and sustaining legacy weapon systems may result in reduced capabilities to meet nuclear deterrence requirements.

INTERCONTINENTAL BALLISTIC MISSILES

The Air Force is challenged with sustaining the aging Minuteman III system while also designing and fielding the Ground Based Strategic Deterrent with no gap in nuclear deterrence or capability. The Minuteman III is a ballistic missile with intercontinental range. These missiles are dispersed in hardened silos throughout the United States to protect against attack and are connected to an underground launch control center through a system of hardened cables. The Minuteman III intercontinental ballistic missile force has remained on continuous, around-the-clock alert since 1970. The Minuteman III system is 39 years past its planned service life.

The Air Force is planning to replace the Minuteman III with the Ground Based Strategic Deterrent starting in 2029, with a plan to reach full operational capability in 2036. When the Air Force released its proposal request for a new intercontinental ballistic missile in July 2019, the Under Secretary of Defense for Acquisition and Sustainment said that there is "no margin" to do another service life extension for the Minuteman III.[65]

During a January 2020 panel discussion on nuclear modernization, the Air Force Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration echoed the Under Secretary's comments and stated that the Air Force has "been able to sustain [the Minuteman III] and we're going to be able to sustain it until we bring [Ground Based Strategic Deterrent] online, but the margin is very slim." In March 2020, the Government Accountability Office determined that if the Ground Based Strategic Deterrent program suffers any delays, the Air Force could find itself with logistical problems.[66] The Government Accountability Office and the DoD OIG have reported sustainment challenges for the Minuteman III system related to aging facilities and communications equipment, launch infrastructure, and obsolete parts.

Another challenge impacting the modernization effort is the DoD budget. According to the Congressional Research Service, the cost of the Ground Based Strategic Deterrent program will rise rapidly from $570.4 million in FY 2020 to $3 billion in FY 2023.[67] The DoD's Office of Cost

[64] Congressional Research Service, "Navy *Columbia* (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress," updated February 26, 2020.

[65] Report No. GAO 13-831, "ICBM Modernization: Approaches to Basing Options and Interoperable Warhead Designs Need Better Planning and Synchronization." September 20, 2013.

[66] Report No. GAO 20-296, "Defense Nuclear Enterprise: Systems Face Sustainment Challenges, and Actions Are Needed to Effectively Monitor Efforts to Improve the Enterprise," March 26, 2020.

[67] Congressional Research Service, "U.S. Strategic Nuclear Forces: Background, Developments, and Issues," January 3, 2020.

The ballistic-missile submarine USS Maine (SSBN 741) returns to service in Silverdale, Washington, May 2, 2020. (U.S. Navy photo)

Assessment and Program Evaluation estimates the total cost at $85 billion. The Air Force had previously stated it would cost $65 billion; however, other estimates project the price tag as high as $150 billion. Properly budgeting, procuring, and deploying the Ground Based Strategic Deterrent while also maintaining the aging systems will challenge the DoD, but are critical to assuring nuclear deterrence.

STRATEGIC BOMBERS

Similar to the sea-based and land-based legs of the nuclear triad, the air-based leg of the triad also faces modernization and sustainment issues. The DoD currently deploys two types of strategic bombers—the B-2 and B-52—that can deliver nuclear weapons. The Air Force has employed these aircraft in conventional conflicts over the past two decades and upgraded the aircraft to sustain their capabilities. However, these bombers are aging and in high demand.

Air Force officials have stated that sustainment efforts may not be sufficient to meet emerging challenges.[68] The Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics has stated that he is concerned about who will pay the bill for nuclear triad modernization and replacement programs. In addition to the nuclear mission, the B-2 is in need to support conventional bomber missions. The current B-2 operational fleet consists of 20 total aircraft, so the Air Force must carefully manage the timing of maintenance activities, aircraft modifications, programmed depot maintenance, assignment of a flight test aircraft, and the flying-hour program.[69] The smaller fleet size also affects the ability to conduct tests to ensure the bombers are able

[68] Congressional Research Service, "U.S. Strategic Nuclear Forces: Background, Developments, and Issues," January 3, 2020.

[69] Report GAO 20-296, "Defense Nuclear Enterprise: Systems Face Sustainment Challenges, and Actions Are Needed to Effectively Monitor Efforts to Improve the Enterprise," March 26, 2020.

to execute their nuclear deterrence mission. During a recent DoD OIG evaluation, the Air Force provided data showing the required number of B-2 aircraft was not being allotted to a joint DoD–Department of Energy testing program. In seven joint DoD–Department of Energy tests conducted from 2004 to 2019, the DoD OIG found five tests were not conducted with the required number of B-2 aircraft.

The current B-52 operational fleet consists of a total of 76 aircraft, including 46 designated as nuclear-capable. The B-52H began operations in 1961, and the B-52 fleet originally had a planned service life of approximately 20 years. However, the Air Force now plans to sustain the B-52 until at least 2050 and has not identified an eventual replacement. During a January 2020 panel discussion on nuclear modernization, the Air Force's Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration stated that the Air Force is working to refurbish its fleet of B-52 bombers with new engines, radars, and other systems. He added that the upgrades will "bring the platform into the 21st century and for some decades to come." In FY 2021, the DoD OIG plans to conduct an audit to determine whether the B-52 bomber modification and modernization plans are being implemented in accordance with the Air Force acquisition strategy.

AIR-LAUNCHED CRUISE MISSILE AND THE LONG-RANGE STANDOFF MISSILE

The Air Force faces challenges developing and fielding the long-range standoff missile while maintaining the existing weapon system. The air-launched cruise missile, first operational in 1982, is a long-range self-guided missile with a nuclear warhead that is carried by the B-52 bomber. The missile had an original planned service life of 10 years, meaning it is more than 20 years past its planned service life. The air-launched cruise missile has experienced issues with multiple aging subsystems. According to the Government Accountability Office, weapons integration equipment, pylons, launchers, common support equipment, air-launched cruise missile-peculiar support equipment, and automated test equipment all have aging and supportability issues that require assessment and actions. The Air Force Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration stated that the air-launched cruise missile "is 25 years past its service life and we have issues with that from an availability [standpoint] as our stockpile drives down." He also stated, "From a reliability standpoint, it's very old and that reliability continues to go down, and from a survivability standpoint, the [air-launched cruise missile] is losing some of that because our adversaries have developed air defenses" against the missile.

As the replacement for the aging air-launched cruise missile, the long-range standoff missile will provide the B-52 the capability to deliver standoff weapons that can penetrate and survive advanced integrated air defense systems, thus holding targets at risk anywhere on Earth.[70] The long-range standoff program is a joint program between the DoD and the Department of Energy, which is separately managing the related nuclear warhead life extension program. The Government Accountability Office concluded in July 2020 that conducting parallel development, design, and test activities with the Department of Energy to ensure the long-range strike option adequately integrates the Department of Energy–designed warhead will likely be challenging for the program, primarily because of the development of new technologies. Related schedule risks also exist

[70] DoD, "Nuclear Posture Review," 2018.

as delays in either program would likely impact overall long-range standoff missile development and delivery.[71]

Finally, the Air Force does not have sufficient inventory to continue testing the air-launch cruise missile. The longer it takes to field the long-range standoff, the fewer air-launch cruise missiles the Air Force will have in its inventory to continue testing missile effectiveness. The testing employs missiles for live launch and destructive testing, thus reducing the fleet of missiles per year. Air Force officials have noted that the fleet would be sustainable for a longer period if the decision was made to stop testing. However, this would mean that the data collected during the annual tests would no longer be available to predict the life of the missile, and the Air Force would lose full confidence that it could execute the mission of the air-launch cruise missiles.[72] The DoD OIG intends to evaluate how the Air Force plans to balance testing the air-launch cruise missile with sustaining an adequate fleet size until replaced with the long-range standoff. Although senior U.S. officials emphasize that the highest priority of the DoD is deterring nuclear attack and maintaining the nuclear capabilities necessary to do so, the DoD is challenged by balancing the sustainment of current nuclear weapon systems while refurbishing or replacing these systems.

BALLISTIC MISSILE DEFENSE

The proliferation of offensive ballistic and cruise missiles and emerging hypersonic weapon technologies from adversaries presents challenges for the U.S. military's ballistic missile defense capabilities. According to the 2019 Missile Defense Review, the Ballistic Missile Defense System provides active defense of the U.S. homeland and deployed forces, allies, and partners. The system is an integrated, layered architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets.[73]

The DoD must modernize its ballistic missile defense to meet current and emerging threats. However, there is no clear DoD-wide governance structure. Missile defense resources and responsibilities are shared across all DoD combatant commands, each with its own unique requirements. Adversaries' and rogue nations' development of hypersonic and ballistic missile capabilities means the DoD must be prepared and capable of deterring and defeating these missile threats.

GROUND-BASED MIDCOURSE DEFENSE

The Ground-Based Midcourse Defense element of the Ballistic Missile Defense System provides the combatant commanders with the capability to engage and destroy intermediate-range and long-range ballistic missile threats in space to protect the United States. There are a limited number of ground-based interceptors in the U.S. inventory, and multiple interceptors may be required to counter each incoming warhead. Because of the low number of interceptors, a second layer of missile defense is necessary to destroy remaining warheads that are not destroyed by the Ground-Based Midcourse Defense system. Additionally, replacing the Ground-Based Midcourse Defense system is another challenge the DoD must address. Adding to this challenge is the fact that the DoD canceled the Redesigned Kill Vehicle

[71] Report No. GAO 20-409, "Nuclear Weapons: Actions Needed to Address the W80-4 Warhead Program's Schedule Constraints," July 24, 2020.

[72] Report No. GAO 20-296, "Defense Nuclear Enterprise: Systems Face Sustainment Challenges, and Actions Are Needed to Effectively Monitor Efforts to Improve the Enterprise," March 26, 2020.

[73] DoD, "Missile Defense Review," 2019.

program due to technical design problems in 2019. This program was intended to meet emerging ballistic missile threats, and it is unclear what the replacement will be.

AEGIS BALLISTIC MISSILE DEFENSE SYSTEM

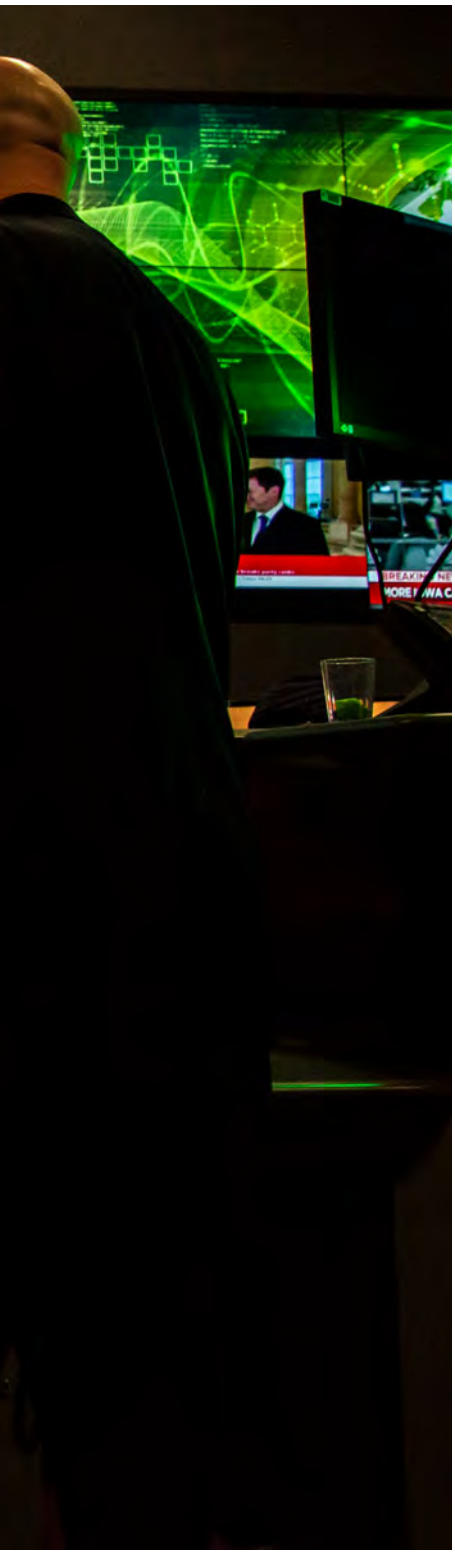
The Aegis Ballistic Missile Defense System is the naval component of the Missile Defense Agency's Missile Defense System and uses ship and ground-based systems to engage short-range to intermediate-range ballistic missiles. A small number of Navy cruisers and destroyers in the Pacific and Atlantic fleets are equipped with Aegis ballistic missile defense. In response to increasing demand from the combatant commanders for ballistic missile defense, the Missile Defense Agency and Navy are working together to increase the number of Aegis ballistic missile defense–capable ships. However, a former Chief of Naval Operations stated that the ballistic missile defense mission is straining the Navy's hard-worn surface combatants and was a factor in the degraded readiness in the surface fleet. At a 2018 U.S. Naval War College's Current Strategy Forum, he stated, "Amid the nuclear threat from North Korea, the ballistic missile defense mission began eating more and more of the readiness generated in the Japan-based U.S. 7th Fleet, which created a pressurized situation that caused leaders in the Pacific to cut corners and sacrifice training time for their crews, an environment described in the Navy's comprehensive review into the two collisions that claimed the lives of 17 sailors in the disastrous summer of 2017."

The Aegis Ashore program is the land-based component of the Aegis Ballistic Missile Defense System with deckhouses and launchers that are nearly identical to the versions aboard Aegis Ballistic Missile Defense ships. While a site has been built and is operational in Romania, construction and contract performance issues have delayed the initial operating capability of a site in Poland, which is central to plans for the defense of Europe and U.S. allies in the region. In March 2020, the Missile Defense Director testified that the Missile Defense Agency had to request $96 million in additional funds to complete the project, which was originally supposed to be certified as operational in 2018. The Director also stated that the contractor did not provide an accurate account of updates to systems integral to installing the weapon systems, such as heating, cooling, power, and auxiliary. In FY 2021, the DoD OIG plans on evaluating the impact from construction delays on the Aegis Ashore system in Poland and whether the site will still be able to meet operational requirements.

CONCLUSION

Assuring space dominance, nuclear deterrence, and missile defense presents significant challenges for the DoD. Near-peer competitors and rogue nations are investing in their own capabilities to protect their interests and deter or defeat U.S. capabilities. With the establishment of Space Force, the DoD acknowledged the strategic importance of space as a warfighting domain and its critical role in effectively deterring nuclear weapons and defending against ballistic missile threats. The DoD is also working to maintain the aging nuclear triad while developing and deploying modern replacements without compromising coverage in the U.S. military's deterrent capabilities. Finally, the growing threats of hypersonic and ballistic missiles require increasing DoD capabilities to protect U.S. interests around the world. The DoD must balance the growing threats in these key areas while ensuring it is modernizing the capabilities without compromising its dominance and current deterrent capability.

Marines with Marine Corps Forces Cyberspace Command in the cyber operations center at Lasswell Hall on Fort Meade, Maryland, February 5, 2020. (U.S. Marine Corps photo illustration)



Challenge 5. Enhancing Cyberspace Operations and Capabilities and Securing the DoD's Information Systems, Networks, and Data

INTRODUCTION AND OVERVIEW

The DoD depends on cyberspace and cyber capabilities to conduct and support its business and military operations across all domains—land, sea, air, space, and cyberspace. Cyberspace is defined as a global domain consisting of the Internet, telecommunications networks, and computer systems. Cyber capabilities are devices or software used to achieve military objectives in and through cyberspace. The 2019 National Intelligence Strategy identifies cyber threats as one of the most significant threats to U.S. national security. The DoD continues to face sophisticated and evolving cyber attacks from malicious actors such as nation-states (Russia, China, Iran, and North Korea), terrorist groups, hacktivists, and other independent malicious actors. These adversaries are constantly attempting to exploit DoD cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target DoD critical infrastructures, and manipulate information.

To protect the DoD Information Network (DODIN) from cyber threats, the DoD must continuously assess, acquire, and adapt its cyberspace capabilities and employ a skilled cyber workforce to defend the DODIN, as well as the networks and systems operated by non-DoD entities, the Defense Industrial Base, and U.S. allies. The DODIN is a set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand for service members, policymakers, and support personnel, whether interconnected or stand-alone. The DODIN consists of all networks owned or leased by the DoD. The 2019 DoD Digital Modernization Strategy focuses on increasing DoD-wide technological capabilities and adopting enterprise systems through four strategic initiatives—innovation, optimization, cybersecurity resiliency, and talent cultivation. Deterring and defeating cyber threats requires the DoD to continue improving its cyberspace operations in these four areas.

COORDINATING EFFECTIVE CYBERSPACE OPERATIONS

At a September 2019 cybersecurity summit, the Secretary of Defense noted that cyber is part of a hybrid war that blurs the lines between peace and wartime. Although not at war, many nation-states, such as China, Russia, North Korea, and Iran, engage the United States and its allies in cyberspace below the threshold of armed conflict. To counter these threats, the 2018 DoD Cyber Strategy calls for the DoD to "defend forward" by disrupting or halting malicious cyber activity at its source. Defending forward can be described as the DoD working on foreign networks to prevent attacks before they happen through persistent engagement of the adversary, wherever the adversary is located. This often requires highly coordinated cyberspace operations that involve multiple agencies and military commands. As nation-state threats continue to increase, the importance of the DoD's ability to coordinate effective cyberspace operations will only continue to grow.

DEVELOPING THE TOOLS AND CAPABILITIES TO DEFEND FORWARD

As the DoD disrupts or halts malicious cyber activity at its source, the DoD must also continue focusing its efforts on the required tools and capabilities that support both offensive and defensive cyberspace operations. Properly understanding and including cyberspace operations requirements during the acquisition process, such as a cost estimate informed by an independent analysis assessment, is critical to effectively executing cyberspace operations. The DoD awarded a contract in 2018 to build a better integrated systems architecture to address the challenges of coordinating offensive and defensive cyberspace operations across multiple platforms. Run by the Air Force, the Unified Platform is designed to consolidate and standardize the variety of big data used by the U.S. Cyber Command (USCYBERCOM) and its subordinate commands. The Unified Platform is part of USCYBERCOM's Joint Cyber Warfighting Architecture, which is intended to guide the development and prioritization of cyberspace capabilities across the DoD. The Unified Platform's success is vital to the execution of cyberspace and multi-domain operations and is intended to enable global synchronization, integration, and execution of many missions and functions. The Unified Platform is also intended to integrate and analyze data from both offensive and defensive operations jointly with intelligence activities and alliance partners, and provide a rapid prototyping capability for deploying cyber tools quickly to the field.

In June 2020, however, the Government Accountability Office reported that due to evolving USCYBERCOM requirements, the Unified Platform's "cost estimate was more than five times its initial estimate at program initiation, which had not been independently assessed." The Government Accountability Office also found that the program's current approach does not "plan to complete a schedule risk assessment." Instead, the Government Accountability Office found that the prototyping program requires fielding new features every 3 months instead of on a continuous basis, which did not align with the industry's agile practices.[74] The Senate Armed Services Committee has also expressed concern about the appropriate level of oversight and coordination of the Joint Cyber Warfighting Architecture and believes that cyberspace acquisition priorities and objectives must be aligned with

[74] Report No. GAO-20-439, "Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight," June 3, 2020.

USCYBERCOM's mission needs. The DoD must ensure that its cyberspace operations acquisition programs properly determine requirements and cost estimates to ensure the programs are aligned with identified needs. Failing to do so creates unnecessary risk by increasing costs, or more critically, delaying the deployment of programs.

DEFENDING AND SECURING DOD SYSTEMS, NETWORKS, DEVICES, AND DATA

Implementing effective cyber hygiene is a persistent challenge for the DoD because of the size and complexity of the DODIN, the volume of its users, and the mix of classified and legacy information systems, networks, devices, and data. Cyber hygiene is a set of practices and steps followed by system administrations and users, such as identity verification and managing user privileges, which are intended to manage common cybersecurity risks. To complicate matters even more, the coronavirus disease–2019 (COVID-19) pandemic has forced the DoD to provide unprecedented levels of remote access and telecommunication capabilities to support maximum teleworking and facilitate remote network connections to the DODIN for nearly three million Military Service members, civilians, and contractors. These connections from an individual's home network (via secure connection), in addition to other personal and smart devices sharing the same home network, significantly increased the number of potential vulnerabilities and risk of cyber attacks by U.S. adversaries. Good cyber hygiene protects the DODIN and Defense contractors, including the national security information processed and stored by DoD systems, networks, devices, and U.S. allies, while minimizing risks to national security and military and business operations.

STRENGTHENING AND PROTECTING SYSTEMS, NETWORKS, AND DATA

Since 2015, the DoD has worked hard to improve cyber hygiene by identifying and remediating cyber vulnerabilities. However, the oversight community continues to identify challenges to improving cyber hygiene. For example, the Government Accountability Office stated in a 2020 report that cybersecurity experts estimate that 90 percent of cyber attacks could be prevented by implementing basic cyber hygiene controls and sharing best practices.[75] The Government Accountability Office also reported that the DoD has not completed tasks associated with cyber hygiene initiatives dating back to 2015, including some that were supposed to be completed in 2016 and 2018.[76] In 2020, the DoD OIG issued a followup report on corrective actions taken by DoD Components in response to cyber vulnerabilities previously identified. The DoD OIG determined that the DoD Components reviewed did not consistently mitigate vulnerabilities or include unmitigated vulnerabilities in plans of action and milestones.[77] The DoD OIG intends to conduct an audit in FY 2021 to determine the extent to which the DoD's vulnerability identification and mitigation programs are coordinated, synchronized, and overseen to maximize program effectiveness.

The DoD continues to face challenges protecting classified information on the DODIN and ensuring that users are not illegally obtaining and providing this information to malicious actors. The DoD has three major initiatives to protect the classified information on the

[75] Report No. GAO-20-241, "Cybersecurity: DoD Needs to Take Decisive Actions to Improve Cyber Hygiene," April 2020.

[76] Ibid.

[77] Report No. DODIG-2020-067, "Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions," March 13, 2020.

DODIN—automated user activity monitoring; the Identity, Credential, and Access Management capability; and the DoD Insider Threat Management and Analysis Center. Like automated user activity monitoring, the Identity, Credential, and Access Management capability is an automated process that encompasses a full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance, and access management control decisions. The DoD Insider Threat Management and Analysis Center acts as the DoD-wide hub for managing and analyzing threats posed by authorized individuals with access to classified information and on the DODIN who intend to do harm to the United States. In January 2020, the DoD OIG announced an audit to determine whether the Center is providing an enterprise-level capability for insider threat information integration and management.

The emergence of increasingly sophisticated threats and the number of reported cyber incidents continues to highlight the urgent need for strong cybersecurity controls and processes. The DoD cannot protect the DODIN from all cyber threats, and must prioritize and protect the most critical systems, networks, and data. The DoD's Risk Management Framework initiative provides a DoD-wide process that integrates activities for selecting, implementing, and monitoring system security controls based on the designated system risk level.

The DoD is increasingly reliant on the private sector and the accumulation of unclassified and Controlled Unclassified Information by the defense contractors, which raises the risk to U.S. national security. In February 2018, the Council of Economic Advisers published a report detailing that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 alone. This extremely high cost further underscores the need for the DoD to protect and secure its systems, networks, and data regardless of where it is stored and processed. In 2019, the DoD OIG found that contractors did not consistently implement DoD-mandated system security controls for safeguarding DoD information.[78]

To successfully detect data exfiltration attempts and respond to cyber incidents, the DoD must efficiently implement security controls and continuously monitor its networks. In March 2020, the DoD OIG found that cybersecurity officials did not implement 9 of the 17 security controls for the Global Command and Control System–Joint, such as access control policy and procedures, vulnerability management, physical access authorization and control, and account management, at seven select critical sites.[79] While this report shows the need for significant improvement in implementing cybersecurity controls over DoD systems and networks, the DoD is taking steps to secure its networks and data. For example, during the Army's virtual Signal Conference in July 2020, the Defense Information Systems Agency Director announced its collaboration with the National Security Agency to deliver guidance to implement zero trust environments where network access is continually authenticated, rather than relying only on an initial login.

Improving basic cyber hygiene and preventing insider threats can produce immediate results while preventing most cyber attacks and unauthorized disclosures. The DoD should

[78] Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 25, 2019.

[79] Report No. DODIG-2020-068, "Audit of Security Controls Over the DoD's Global Command and Control System–Joint Information Technology System," March 20, 2020.

also focus on developing affordable, automated solutions to mitigate cybersecurity risks across the DODIN, the Defense Industrial Base, and U.S. allies.

MODERNIZING LEGACY SYSTEMS, NETWORKS, AND DEVICES

The DoD information technology (IT) systems and infrastructure are aging and need to be modernized to be protected against cybersecurity threats. Integrating new technology into existing DoD systems is essential to maintain network security and improve network capabilities. More significantly, the potential benefits of cloud computing, big data analytics, increased automation, and cognitive computing can only be fully realized with a suitable, modernized, and secure network.

IMPLEMENTING DOD IT MODERNIZATION EFFORTS

The DoD's 2019 Digital Modernization Strategy serves as the DoD's strategic plan for information resource management and presents IT-related modernization goals. The Digital Modernization Strategy states that the DoD requires a modern, "secure, consistent, and cost efficient network to conduct operations and business functions." Utilizing commercial cloud computing and artificial intelligence (AI) are two of the DoD's approaches to modernizing its IT. For example, the DoD is leveraging available commercial cloud computing infrastructure, instead of deploying its own infrastructure, to increase its bandwidth, store and process big data platforms, and implement emerging technologies, such as AI and machine automation.

The transition to the commercial cloud environment, however, presents new security challenges. According to the 2018 DoD Cloud Strategy, the transition from the traditional IT management model (DoD owned and operated) to a managed cloud computing model (commercially leased storage and contracted support) will improve ease of use, automation, adoption of leading-edge technology, and optimize the DoD's information domain. By using the commercial cloud computing model, the DoD shifts some responsibility for cybersecurity and operational support through service-level agreements and contracts to the cloud service providers. The DoD OIG announced an audit in January 2020 to determine whether the DoD Components identified the necessary security controls and ensured that cloud service providers maintained cybersecurity requirements for select cloud computing services.

The DoD Cloud Strategy also focuses on implementing enterprise cloud solutions, such as the Joint Enterprise Defense Infrastructure (JEDI) and the Defense Enterprise Office Solution (DEOS), to support the strategy to acquire and implement enterprise applications and services for joint use across the DoD. However, these contract awards have been challenged and stalled in litigation since 2019, forcing the DoD to leverage existing commercial cloud computing solutions in a decentralized process. The DoD OIG has an ongoing audit to determine whether the DoD Components identified the necessary security controls and ensured that cloud service providers maintained cybersecurity requirements for cloud services.

To accelerate the delivery of AI-enabled capabilities across the DoD, the DoD Chief Information Officer established the Joint Artificial Intelligence Center in 2018. At the September 2020 DoD Artificial Intelligence Symposium and Exposition, the DoD Chief Information Officer stated that the Digital Modernization Strategy provides a framework to harness AI's full potential by bringing together the technological capabilities of AI, cloud computing, data, command and

control, and cybersecurity into a common and modern IT system. The DoD OIG issued a report in 2020 that audited the Joint Artificial Intelligence Center's progress to develop an AI governance and framework. The DoD OIG found that the Joint Artificial Intelligence Center must develop a standard definition of AI, a security classification guide, a process to accurately account for AI projects, the capabilities for sharing data, and the standards for legal and privacy considerations.[80] The DoD OIG also determined that DoD Components and contractors did not consistently implement security controls to protect the data used to support AI projects and technologies from internal and external cyber threats. The DoD must incorporate cybersecurity requirements during the development of new technologies to maintain its technological advantage against its adversaries and malicious actors.

DEVELOPING AND DEPLOYING CYBER SECURE NEW TECHNOLOGIES

While the DoD balances its IT modernization efforts to create a secure and cost-effective IT architecture, it must also continue developing and integrating cutting-edge technology for weapon systems, communications equipment, and intelligence platforms. Cybersecurity must be considered during the technology's design phase, instead of after its development and deployment. Cybersecurity experts believe that more than 80 percent of breaches exploit known vulnerabilities in a software application. Flaws in network architecture and mission software system design can expose existing software weaknesses and degrade the technology's effectiveness. Any of these weaknesses, when exploited by an attacker, can lead to the users' loss of confidence in the technology, degraded lethality, or complete mission failure.

Although the DoD OIG and the Government Accountability Office have warned of cybersecurity risks for decades, the DoD did not effectively prioritize weapon system cybersecurity until recently. Cybersecurity was not always included at the beginning of the life cycle of the application and underlying infrastructure. According to the Office of the Under Secretary of Defense for Research and Engineering, nearly 70 percent of all vulnerabilities are introduced when the system code is written (design phase); however, most vulnerabilities are not identified until the system is connected to other systems to provide full functionality (system integration phase). A collaborative understanding between development and operations staff is necessary to address this gap and ensure software development and IT are integrated during the design phase.

In 2019, the DoD Chief Information Officer released the DoD Enterprise DevSecOps Reference Design document that explained DevSecOps is an "organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec), and operations (Ops)." The DoD Enterprise DevSecOps Reference Design document provides operational guidance to improve the overall design, build, and deployment of cyber-resilient software. The DoD Digital Modernization Strategy adds that DevSecOps ensures that quality assurance and cybersecurity are included in development of software. DevSecOps also provides software assurance and automates the processes between software development, cybersecurity, and IT teams by building cyber-resilient software. Quality assurance is also an important part

[80] Report No. DODIG-2020-098, "Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology," June 29, 2020.

of the software development process to reduce risks and ensure that the software is dependable and trustworthy. Enabling security and functional capabilities to be tested and built simultaneously could lower development cost and deploy secure software at a more rapid pace. To assess the DoD's progress with DevSecOps and software assurance, the DoD OIG began an audit in 2020 to determine whether DoD program management offices implemented software assurance countermeasures to mitigate or remediate the vulnerabilities found in DoD weapon system programs.

BUILDING AND MAINTAINING AN EVOLVING CYBER WORKFORCE

The 2018 DoD Cyber Strategy identifies the cyber workforce as a critical asset, but the DoD faces persistent challenges recruiting, developing, and retaining a skilled cyber workforce of system administrators, software developers, network operations specialists, and system evaluators. The DoD should take appropriate steps to ensure it recruits, retains and develops a skilled cyber workforce to perform cyberspace operations, defend and secure the DODIN, and modernize its IT infrastructure.

In March 2020, the congressionally mandated Cyberspace Solarium Commission stated that the U.S. Government has a shortage of over 33,000 cyber workforce personnel and recommended that agencies identify opportunities and build hiring mechanisms for women and underrepresented communities to deepen and diversify the available cyber workforce candidate pool.[81] The DoD routinely struggles to recruit, retain, and develop the number of cyber professionals needed to conduct offensive and defensive cyberspace operations, such as securing its networks and supporting the Defense Industrial Base and its allies. Although the DoD is adapting to recruiting and training its own cyber warriors (known as Cyber Mission Force), the Military Services anticipate difficulties recruiting and retaining sufficient talent. These difficulties are only compounded by additional challenges diversifying the cyber workforce so it is more inclusive of women and underrepresented communities.

Congress gave the DoD authority in National Defense Authorization Act (NDAA) for 2016 to create the Cyber Excepted Service personnel system. The Cyber Excepted Service personnel system is an enterprise-wide approach for managing civilian cyber professionals that provides the needed flexibility for the recruitment, development, and retention of high-quality cyber professionals. DoD personnel can be converted into the Cyber Excepted Service personnel system, but the program is voluntary and personnel in a competitive service position may decline the conversion. As a result, the DoD Chief Information Officer cannot mandate conversion until the employee vacates his or her position. Since 2017, DoD officials have converted more than 7,400 civilian positions, with a plan to convert an additional 11,300 positions by FY 2022. The voluntary nature of the authority has led to slow program adoption and the limited number of conversions. The DoD OIG has an ongoing audit to determine the extent to which the DoD is meeting Federal requirements and DoD strategic goals for recruiting and retaining its civilian cyber workforce, such as the Cyber Excepted Service personnel system.

In June 2020, the President signed Executive Order 13932, requiring the Federal Government to overhaul its hiring practices. The Executive

[81] United States Cyberspace Solarium Commission, "United States Cyberspace Solarium Commission Report," March 11, 2020.

order emphasizes skills and competency instead of a person's education, expands the universe of qualified candidates, and ensures a more equitable hiring process.[82] In addition, the House of Representatives version, H.R. 6395, of the FY 2021 NDAA has several provisions governing the DoD Chief Information Officer's enterprise cyber talent management. For example, one provision would require that the DoD Chief Information Officer submit a strategy to Congress for how to best expand the DoD cyber workforce's participation in instructional and participatory opportunities, such as GenCyber, which is a program designed to create more cybersecurity awareness among K-12 students to build a larger pool of diverse candidates to serve in the Federal cyber workforce.

To improve the DoD's ability to recruit and retain its cyber workforce, the DoD must first properly identify its cyber workforce requirements. In 2019, the Government Accountability Office determined that the DoD did not appropriately assign work role codes to vacant positions, categorize work codes, or categorize work codes consistent with their position descriptions for its IT management occupational job series. The DoD must accurately categorize all cyber workforce positions in order to effectively identify its critical staffing needs and take advantage of expedited hiring authorities.

Although recruiting and attracting the necessary talent is critical, the DoD must also ensure its cyber workforce is appropriately trained and developed to achieve the DoD's mission. Competing with private industry for competent and skilled cybersecurity professionals further complicates the DoD's ability to retain its cyber workforce. The 2020 Cyberspace Solarium Commission report recommended that the U.S. Government design cybersecurity-specific upskilling and transition assistance programs for veterans and transitioning Military Service members to move into Federal civilian cybersecurity jobs. The report also recommended that the DoD develop management training to cultivate best practices that foster a more diverse cyber workforce and more inclusive work environment, and establish cyber career paths that allow movement between departments and agencies and into senior leadership positions.

The oversight community and Congress recognize the importance of developing and retaining the DoD cyber workforce. In 2019, the Government Accountability Office reported that USCYBERCOM and the Military Services faced challenges related to training cyber warriors, which comprise the Cyber Mission Force, including identifying the numbers of personnel that need to be trained, establishing required independent assessors to ensure consistent Cyber Mission Force training requirements, and establishing training task lists for foundational training courses. In addition, a 2016 DoD OIG report recommended that USCYBERCOM and the Military Services develop a doctrine, organization, training, material, leadership and education, personnel, facilities, and policy framework that addresses strategies to build, grow, and sustain the Cyber Mission Force.[83] As of March 31, 2020, more than 4 years later, USCYBERCOM and the Marine Corps have yet to develop such a strategy, adversely impacting the DoD's ability to retain a skilled force.

[82] Executive Order 13932, "Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates," June 26, 2020.

[83] Report No. DODIG-2016-026, "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions," November 24, 2015.

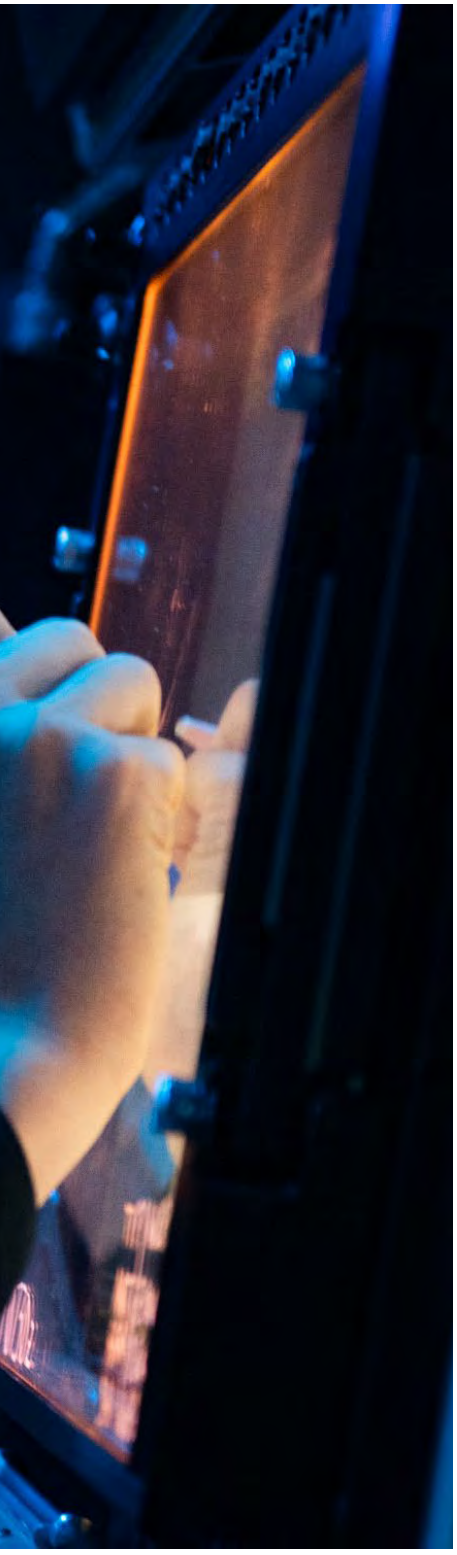
In the FY 2020 NDAA, Congress directed the DoD to conduct a review of DoD cyber and IT personnel to improve the development and training provided to the cyber workforce. The review should determine the optimal strategy to develop the structure of the DoD cyber workforce, as well as assess the training and capability needs of the Cyber Mission Force. The DoD cyber workforce must be appropriately resourced and enabled with right capabilities to support current and future cyberspace missions, identify critical network vulnerabilities, and limit malicious actors from compromising DoD operations.

The DoD is also pursuing several training initiatives to improve the development of its cyber workforce, such as deploying the Persistent Cyber Training Environment. The Persistent Cyber Training Environment initiative is a virtual training platform that allows the DoD cyber workforce to conduct individual or collective cyber training and mission rehearsals worldwide, regardless of geographic location. The Training Environment leverages existing network connectivity to facilitate sharing resources; enable realistic training with variable conditions to increase readiness and effectiveness of the cyber workforce; and enhance training management by standardizing, simplifying, and automating processes. In June 2020, USCYBERCOM performed a virtual exercise, using the training environment "Cyber Forge," despite the challenges of operating remotely during the COVID-19 pandemic. The DoD plans to expand this training environment and make it the primary tool to train and assess its personnel, with the goal of using it for USCYBERCOM's premier annual exercise "Cyber Flag." To assess the DoD's training initiatives for the cyber workforce, the DoD OIG intends to conduct an audit to determine the effectiveness of the combatant commands' exercises to simulate operations in a disrupted, degraded, or contested cyberspace environment.

CONCLUSION

DoD innovation is key to future readiness as well as developing and delivering technology to the military. To successfully modernize and develop cyber-resilient systems, networks, and devices, the DoD will need to rely heavily on its cyber workforce, which must adapt to meet the needs of today and the future. The DoD must continuously identify, address, and adapt to evolving challenges affecting its ability to protect the DODIN and conduct cyberspace operations. The DoD must also improve its basic cyber hygiene and monitoring for potential threats, to prevent unauthorized disclosures that could adversely affect U.S. national security. This will require the DoD to clarify its cyber roles, increase its capability to conduct multi-domain operations, improve cyber workforce readiness, and use advanced autonomous tools to defend the DODIN and conduct cyberspace operations.

A U.S. Navy Operations Specialist 3rd Class stands watch as a surface radar controller in the combat information center aboard the Ticonderoga-class guided-missile cruiser USS Antietam (CG 54). (U.S. Navy photo)



Challenge 6. Transforming Data Into a Strategic Asset

INTRODUCTION AND OVERVIEW

Valuable and actionable information derived from raw data is a strategic asset integral to the U.S. military's ability to preserve and expand its competitive advantage and defend the United States. In 2017, the Secretary of Defense designated information as a joint function, critical to the planning and employment of the Joint Force, along with command and control, intelligence, fires (or using weapons for effects on a target), movement and maneuver, protection, and sustainment.[84] In February 2020, the Navy released its Information Superiority Vision acknowledging that "Information is Combat Power." However, despite these statements, the DoD is challenged to fully understand the universe of data and information collected, stored, and analyzed on thousands of operational systems, servers, and millions of computers, information technology (IT) devices, and mobile devices.[85]

Data, data systems, and information permeate every aspect of the DoD. The Office of the Chief Information Officer defines data as "the representation of information in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means," and states that data is "concerned with the encoding of information for repeatability, meaning, and proceduralized use." Information is defined as "the state of a something-of-interest that is materialized, in any medium or form, and communicated or received" with the emphasis on what the information means, who uses it, and why it is of interest. However, multiple challenges remain in efficiently using the data systems and turning data into valuable and actionable information for decision makers at all levels. These challenges focus on the volume, velocity, variety, and veracity of the data. The DoD is working to address these challenges through full-spectrum data management strategies and plans, coupled with effective, comprehensive governance, standardization, and funding, to transform data and information into strategic assets.

[84] Department of the Navy, "Information Superiority Vision," February 14, 2020. Secretary of Defense Memorandum on Information as Joint Function, September 15, 2017.

[85] DoD, "DoD Digital Modernization Strategy 2019," July 12, 2019.

INFORMATION AS STRATEGIC ASSET

For data to be valuable and actionable for decision makers, it must be "visible, accessible, understandable, trusted, and interoperable." When data is reliable, accessible, and properly used, the information becomes a powerful tool for decision makers.

Senior DoD leaders recognize the critical role data and information play in U.S. military operations. The DoD Chief Information Officer has said that data is the fuel and engine for everything the DoD must do to bring intelligence and operations together, providing all-domain situational awareness. Senior leaders also recognize the potential that data has to change how war is conducted. At the 2019 Association of the U.S. Army annual conference, the Secretary of the Army stated, "Big data and network security become the next battlefield. If we do not have a system in place, access to the data becomes our no man's land." Key DoD documents also recognize the importance of data and information. For example, the 2018 National Defense Strategy highlights advanced computing and "big data" analytics as two of the new technologies that are changing society and, ultimately, the character of war. The Strategy also recognizes that a "modern, agile, information-advantaged Department requires a motivated, diverse, and highly skilled civilian workforce, [including] information experts, data scientists, computer programmers, and basic science researchers and engineers—to use information, not simply to manage it."

Elevating the importance of data and information in military operations impacts all aspects of doctrine, organization, training, material, leadership, education, personnel, facilities, and policy. For example, acknowledging that "Information is Combat Power," drove the Joint Staff to update its doctrine and publications. In 2017 and 2018, the Joint Staff updated Joint Publication 1-0, "Doctrine of the Armed Forces," and Joint Publication 3-0, "Joint Operations," stating that the information function "encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making."[86]

In 2019, the DoD published the first-ever DoD Digital Modernization Strategy, which acknowledged that "agile, resilient, transparent, seamless and secure IT infrastructure and services, that transform data into actionable information and ensure dependable mission execution … are vital." The Strategy also states that the DoD should "treat information as a strategic asset" and tasks the Chief Information Officer with the responsibility for ensuring "that innovative information capabilities are available throughout all areas of DoD supporting warfighting, business, and intelligence missions."

DATA CHALLENGES

The challenges to effectively using data are numerous and compounded by the vast quantity of data collected, the decentralized nature of operations, and disparate funding streams within the DoD. The DoD has approximately 10,000 operational systems, each with thousands of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands

[86] Joint Chiefs of Staff, Joint Publication 1, "Doctrine for the Armed Forces," March 25, 2013, incorporating change 1, July 12, 2017; Joint Publication 3-0, "Joint Operations," January 17, 2017, incorporating change 1, October 22, 2018.

of commercial mobile devices. Each system has its own team, requirement, budget, and customers. As the DoD Chief Data Officer stated in November 2019, "Every one of those systems was put in place by a different team of people, meeting a different set of requirements, with a different budget, for different customers, in a different place, over a time scale of 60 years of IT. It's like working in an archaeological dig."

For more than two decades, the number of laws, rules, and regulations governing the collection, use, and protection of data and information have created a significant challenge for the DoD. The various laws and rules have created overlapping layers of standards and accountability, making it difficult to discern which rules and regulations apply to each data set and system. In FY 2021, the DoD OIG intends to conduct an audit to determine the effectiveness of the DoD's information security policies, procedures, and practices.

In 2002, the DoD published a directive requiring that "data and information be structured to enable full interoperability and integration across DoD operations and activities" and an "integrated DoD architecture."[87] Although this Directive was published 18 years ago, the DoD still has thousands of different systems that are not fully interoperable across the DoD business enterprise (such as finance, logistics, and human resources).

While earlier laws focused on the integration and security of IT systems, recent legislation, such as the Foundations for Evidence-Based Policymaking Act of 2018, recognizes that data is an asset to be treated distinctly from the IT systems that house it. The Act specifically requires the head of each agency, such as the Secretary of Defense, to submit an annual plan to the Office of Management and Budget and Congress. The plan must identify the data the agency intends to collect, use, or acquire in policymaking and describe how the agency will accomplish data-informed and evidence-based decision making. The Act also established evaluations officers to coordinate agency evidence-building activities.

VOLUME OF DATA

Data is created every single second of every day. As the volume and velocity of data production increase, ensuring the DoD is able to process it becomes a challenge. According to computer scientists at Sandia National Laboratories, "The amount of data produced by sensors and social media is booming—every day there's about 2.5 quintillion (or 2.5 billion billion) bytes of data generated. … About 90 percent of all data has been generated in the last 2 years—there's more data than we have people to analyze. … Intelligence communities are basically overwhelmed, and the problem is that you end up with a lot of data sitting on disks that could get overlooked." If the DoD is unable to process all the data collected, the DoD may miss an opportunity to take advantage of a critical piece of information.

Not all data is useful data. During a February 2020 meeting with data analytics experts, the Deputy Secretary of Defense stated that the DoD must "determine internal methods of data identification, collection, organization and how it can be used most effectively for operational and business decisions." Information governance is the framework of data rules and organizational role delegations that effectively identifies, curates, manages, and secures the best possible data inputs.

[87] DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002.

The volume and diverse sources of data create challenges for the DoD to fully understand all the data it has collected and stored. The FY 2020 National Defense Authorization Act required the DoD Chief Information Officer have access to all DoD data, rules, and regulations. This change alone cannot create effective data governance sufficient to transform data into a strategic asset. Achieving comprehensive control and strategic use of the data collected by the DoD requires strong senior leader support, sufficient resources, and the development of a plan for evidence-based policymaking.

The quantity of data and devices demands accountability at all levels of the DoD to harness and effectively use the vast amounts of expanding data. Managers must be accountable for both their data and their data systems. In addition to knowing what information the DoD has and where the DoD has it, roles and responsibilities must be clearly delineated for data collection, maintenance, and security, as well as data systems, to ensure accountability.

VELOCITY OF DATA

Collecting and analyzing vast amounts of data, whether from open or classified sources, requires the right analytical tools and skilled personnel. At a nuclear deterrence forum in April 2020, the Commander of Air Force Global Strike Command stated that he would prefer to spend one more dollar on "building the best data lake and analytical tools" instead of more bombers or missiles. An interconnected network connects numerous devices capable of creating and accessing data—such as tablets, mobile phones, and social media outlets—and shares the data. This interconnected network has been called the "Internet of Things."

The DoD Digital Modernization Strategy states that the "Internet of Things" is "significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to its user, but it is now connected to surrounding objects and database data." Whether it is data analytics, sensors, or devices, the Strategy states that this interconnected network enables technology to gain the ability to sense, predict, and respond to the DoD's needs. Users and devices are connected and able to rapidly share data with other devices and systems. Exchanging data and using emerging technologies, such as artificial intelligence and machine learning, can be integrated into DoD decision-making processes, changing existing behaviors and speeding up the processing and analyzing of information. Furthermore, speed and connectivity can reduce waste and costs, while also limiting the loss of data. To maintain the speed of information, the DoD must also know what devices need to be replaced, repaired, or recalled.

Artificial intelligence and machine learning present technological opportunities to rapidly process new data created and the DoD must effectively take advantage of their potential benefits. The DoD's challenges related to artificial intelligence are discussed further in Management Challenge 2, "Building and Sustaining the DoD's Technological Dominance," and Management Challenge 8, "Strengthening and Securing the DoD Supply Chain and the Defense Industrial Base."

VARIETY OF DATA

Whether created by humans or machines, data is varied, and includes structured data, such as sensor outputs and spreadsheets, and unstructured data, such as e-mails, texts, voicemails, and audio recordings. The data can be so varied that it must be classified into appropriate categories to be useful. Failure to understand and sort through the variety of data

complicates the DoD's ability to make sense of and analyze the data, potentially creating unnecessary redundancy. Knowing types and categories of data, and having the tools available to sort and use the data, is critical. Redundant data collection, maintenance, and security are inefficient and costly, both in terms of money and time. The DoD must address and reduce redundancy in data and IT to ensure the validity and value of the data, as well as identify potential cost savings.

Congress has required the DoD Chief Information Officer to establish data standards and ensure interoperable systems throughout the DoD to eliminate the unnecessary costs and efforts inherent in redundant data sets and incompatible systems. The Joint Staff is "driving development of data standards supporting interoperability," according to the DoD Modernization Strategy.[88] At a September 2020 Defense Innovation Unit event, the Vice Chairman of the Joint Chiefs of Staff said that in 2021 the DoD is looking at how to better sort, catalog, and exploit data by changing how joint requirements for data and software are developed through the Joint Requirements Oversight Council and then pushed o the Military Services. Standardizing how the data is collected and stored could facilitate DoD efforts to identify the best IT solutions. These solutions could create efficiencies that improve the information's value to senior leaders and facilitate the DoD's business transformation.

The challenges of redundancy, standardization, and interoperability are further complicated by a relatively flat budget for IT that is spread across thousands of funding lines across the DoD. Due to the numerous funding lines, the DoD faces difficulties identifying opportunities to effectively reform and achieve efficiencies. The FY 2021 budget request reflects a 1.64-percent increase of $0.85 billion, compared to FY 2020 enacted levels. Table 2 shows the DoD's IT budget request, which is allocated across the National Defense Strategy's three lines of efforts.

Although reforming business processes is a top DoD priority, only $160 million, or less than one-half of 1 percent, of the $37.7 billion in the FY 2021 budget request for IT was identified to support reform. Creating the standardized systems that categorize the variety of data could minimize redundancy and improve

Table 2. DoD IT Budget Allocation Across Lines of Efforts

Strategic Goal	FY 2019	FY 2020	FY 2021
Rebuilding military readiness as we build a more lethal force	$29.93 B	$31.3 B	$32.2 B
Strengthening alliances as we attract new partners	5.26 B	5.17 B	5.34 B
Reforming the DoD's business practices for greater performance and affordability	0.15 B	0.16 B	0.16 B
Total	**$35.3 B**	**$36.6 B**	**$37.7 B**

Note: Unclassified Submission Only. B represents billions.

Source: DoD Information Technology and Cyberspace Activities Budget Overview, FY 2021 Budget Estimates, February 2020, CAPE.

[88] DoD, "DoD Digital Modernization Strategy 2019," July 12, 2019.

accountability. These are critical investments for the DoD to improve how it does business and speed up its decision making. Effectively investing in reforming the DoD's business processes is one step toward addressing the variety of data, as well as the volume and velocity, and turning it into verifiable and valuable information.

VERACITY OF DATA

Data must be of appropriate utility, integrity, and objectivity to be reliable. The importance and challenge of data quality is not unique to the DoD. A 2017 Harvard Business Review study found that the problem of data quality was "severe," with only 3 percent of the 75 business executives surveyed rating their data quality as "acceptable." Low-quality data, whether entered incorrectly by accident or as disinformation corrupted by an adversary, is an obstacle to actionable information for decision makers. Data quality is critical to ensuring the information presented to decision makers can be trusted and acted upon. For example, in 2020, the DoD OIG determined that the DoD submitted inaccurate financial and award data for publication on USAspending.gov.[89] Failure to provide complete and accurate information, in this case, prevents taxpayers and policymakers from effectively tracking Federal spending and undermines the DATA Act objective of providing quality and transparent Federal spending data publication on USAspending.gov.

Data is such an important strategic asset that adversaries and competitors steal or manipulate data to counter U.S. military capabilities. The Senior Military Advisor for DoD Cyber Policy has noted that adversaries, such as Russia and China, attack the information domain, whether through disrupting data quality using disinformation or attacking the system to steal intellectual property.

The need for proper maintenance and security of both data and data systems cannot be overstated. Failure to protect and maintain data could compromise data integrity and render it of little or no value to the DoD, or worse, leave the U.S. Government and military vulnerable to attacks by adversaries, competitors, rogue nations, or individual actors. The DoD's challenges in cyberspace and in securing DoD networks are discussed further in Management Challenge 5, "Enhancing Cyberspace Operations and Capabilities and Securing the DoD's Information Systems, Networks, and Data."

VALUE OF DATA

To effectively leverage data, it must be turned into valuable information that enables decision makers to optimize processes, improve security, or predict the next event, such as a pandemic or potential national security threat. However, turning data into a valuable information requires a culture that understands, implements, and promotes data-informed decision making, and a workforce that is trained and empowered to collect, integrate, and analyze the data—all in accordance with laws, regulations, and ethical standards.

In November 2019, the DoD Chief Data Officer stated, "People want to talk about technology and really cool tools, and they are wonderful tools … but if we don't start from a cultural change, we're not going to get where we need to go. The Department of Defense does not have a culture of data-centric decision making." The June 2020 announcement transferring the Chief Data Officer to the Office of the Chief Information Officer stated that the role of the Chief Data Officer was to "accelerate the

[89] Report No. DODIG 2020-010, "Audit of DoD Compliance With the Digital Accountability and Transparency Act of 2014," November 19, 2019.

A project officer with the Naval Supply Systems Command (NAVSUP) Business Systems Center (BSC). NAVSUP BSC provides the Navy with information systems support through the design, development, and maintenance of information systems in the functional areas of logistics, supply chain management, transportation, finance, and accounting. (U.S. Navy photo illustration)

transition to a data-driven culture" across the DoD. The 2020 Federal Data Strategy Plan lists 10 ways to build a culture that values data and promotes its use, including investing in continuous and collaborative learning, developing data leaders at all levels of the workforce, and practicing accountability to assign responsibilities and learn from results.[90]

Creating and establishing a culture that understands the value of data and demonstrates comfort with data-driven systems and decision making can assist DoD senior leaders in making critical decisions regarding resourcing priorities and military requirements. For example, in 2019 the Government Accountability Office determined that the DoD's analytic approach—Support for Strategic Analysis—used by the Military Services to evaluate their force structure needs and inform their budget requests was cumbersome, inflexible, did not test assumptions, and lacked joint analytic capabilities to assess force structure.[91] The DoD recognizes the challenges, and efforts are underway to identify alternatives.

Employing the appropriate expertise in all aspects of data and data systems, from IT specialists to data scientists, is another critical challenge for the DoD. In addition to creating a culture of data-informed decision making, the entire DoD workforce, especially

[90] President's Management Agenda, "Federal Data Strategy: 2020 Action Plan," May 14, 2020.

[91] Report No. GAO 19-385, "Revised Analytic Approach Needed to Support Force Structure Decision-Making," March 14, 2019.

A Logistics Data Analysis Center (LDAC) Director highlights the organization's mission. Previously known as Logistics Support Activity, LDAC supports the Army Materiel Command. (U.S. Army photo)

leaders, must also develop a requisite level of comfort and data literacy to properly collect, understand, manage, and employ this asset within their areas of responsibility. The DoD Modernization Strategy recognizes the importance of cultivating a talented and digitally ready workforce as one of its goals. The Strategy states that the competition for a high-quality, experienced workforce is "constant and increasingly aggressive."[92] However, the Strategy confines the importance of a digital workforce to the Cyber Workforce and limits the potential of developing the entire DoD workforce to comfortably understand and use data and information in their jobs.

DoD Components recognize the importance of recruiting, training, and retaining a skilled workforce. For example, the Army's Functional Area 49 branch consists of operations research/systems analysts who are considered the data scientists of the Army. According to the Department of the Army Pamphlet 600-3, the branch produces officers with skills to "introduce quantitative and qualitative analysis to the military's decision making processes" using probability models, statistics, and simulations. Operations research/systems analysis personnel are used across the spectrum of military fields, from personnel management, system acquisition, and resource management, to doctrine and force development, training, and tactical, operational, and strategic planning. The Army's Functional Area 49 Executive Agent noted in a July 2019 memorandum that the branch's core mission is "to help leaders make decisions" with

[92] DoD, "DoD Digital Modernization Strategy 2019," July 12, 2019.

the right tools, whether "advanced data science and machine learning or simple sketch," that translate the "analysis into knowledge that the decision maker understands."

Ethical conduct must be woven into the collection and use of data, to protect and serve the public good. The DoD's unique ability to access and use extraordinary amounts of sensitive data must be tempered by ethical considerations, such as protecting individual privacy rights and civil liberties and ensuring appropriate access and use, when formulating governance policies.

For example, data and information can be used to help the military with recruitment and accessions. With all the data and information the DoD can collect, ensuring it protects personally identifiable information in accordance with the Privacy Act of 1974 and other applicable implementation guidance is critical to demonstrating ethical use and maintaining the public's trust. As the RAND Corporation recently found in a 2019 report, data-driven outreach and recruiting strategies can "help target prospective hires who are more likely to join and fit with one's organization; identify information concerning their interests, needs, and questions; and choose the right places and times to provide that information during their decision process."[93] The report noted that the Military Services and the Joint Advertising Market Research and Studies are "using data-enabled outreach and recruiting strategies to help locate youth who may be qualified for and interested in military service and to recruit them." Data is used to identify priorities, trends, and analysis to inform recruitment decisions, from manpower and funding to shaping messages and identifying target audiences.

The Federal Data Strategy identifies the critical role of ethical governance in its principles and calls on U.S. Government agencies to uphold ethics through checks and balances, effective data stewardship, and transparency through documented processes to engender public trust. The DoD's challenges regarding ethical conduct and decision making are discussed further in Management Challenge 10, "Promoting Ethical Conduct and Decision Making."

CONCLUSION

Addressing the challenges of volume, velocity, variety, and veracity of data requires the DoD to develop policies and interoperable systems to improve decision making and realize efficiencies. The "Internet of Things" and the daily creation of quintillion bytes of data mean the volume of data will not shrink and the velocity will not slow. The diffusion of the DoD IT budget across the DoD Components further exacerbates the challenge of streamlining systems, reducing the duplication of systems, and securely storing the data and information. The DoD must ensure the veracity and quality of its data can be trusted, through standardizing systems, improving interoperability, and ensuring security of data from internal or external threats. Cultivating a culture that understands how to use data, recruiting and retaining the right skills for data management and analysis, and training the DoD workforce are critical to increasing data-driven decision making in the DoD. Transforming data into valuable information for senior decision makers requires the DoD to effectively integrate the volume, velocity, variety, and veracity of data and information into real-time operational decision making and management.

[93] RAND Corporation, "Leveraging Big Data Analytics to Improve Military Recruiting," 2019.

A phlebotomist assigned to Naval Medical Center San Diego, inserts a needle into the arm of a Sailor assigned to the aircraft carrier USS Theodore Roosevelt (CVN 71), in order to donate COVID-19 convalescent plasma at the hospital's Armed Services Blood Program Blood Donation Center August 19, 2020. (U.S. Navy photo)

Challenge 7. Ensuring Health and Safety of Military Personnel, Retirees, and Their Families

INTRODUCTION AND OVERVIEW

Ensuring the health and safety of service members, retirees, and their families is a priority for the DoD. Personnel are the DoD's most critical resource, so it is essential they have the support needed to successfully navigate the challenges of military life. The DoD has experienced a number of challenges maintaining adequate access to high-quality health care, especially as the DoD implements statutory Military Health System reform. There are also challenges related to policy matters; medical records integration with the Department of Veterans Affairs; safeguarding, access, and accuracy of electronic health records; and availability of medical services. In addition, behavioral health issues, such as substance abuse and suicide, remain key health and safety challenges. Finally, environmental health and military housing conditions present serious concerns for the health, safety, and morale of DoD personnel and their families.

While this year's challenge focuses on the areas mentioned above, some management challenges noted in prior years continue to persist, such as child care, sexual assault and prevention, and the increasing costs and fraud related to health care. The DoD's challenge in addressing sexual assault prevention and response is discussed further in Management Challenge 10, "Promoting Ethical Conduct and Decision Making."

MAINTAINING ACCESS TO HIGH-QUALITY AND SAFE HEALTH CARE DURING REFORM

The DoD faces major challenges as the Defense Health Agency assumes responsibility for DoD medical treatment facilities. The Military Health System continues to implement significant reforms in response to congressional requirements in the National Defense Authorization Act (NDAA) for FYs 2017 and 2019, and DoD-wide efforts to improve business processes. In October 2019, the Defense Health Agency assumed administration and management responsibilities for the DoD medical treatment facilities in the United States from the Military Departments. The objective of these reforms is to standardize business and clinical processes, eliminate silos of military health, improve medical readiness, and maintain quality and accessible health

care for the 9.5 million eligible Military Health System beneficiaries. After the transition to the Defense Health Agency, the Military Service Medical Departments' focus will be personnel medical readiness and the responsibilities related to staffing, training, and equipping military medical personnel to provide medical services in an operational setting.

The Defense Health Agency has implemented a phased approach to the transition, relying on support from the Military Departments to administer the DoD medical treatment facilities, while the Defense Health Agency establishes local market offices to support the DoD medical treatment facilities and ensure compliance with Defense Health Agency policy. The FY 2019 NDAA requires the Defense Health Agency to assume administration and management of overseas DoD medical treatment facilities in October 2021.

As part of the transition, the Defense Health Agency plans to close and restructure some DoD medical treatment facilities while relying on the purchased care system (TRICARE) to provide a greater amount of primary and specialty care to beneficiaries. However, a May 2020 Government Accountability Office report cited flaws in the DoD's methodology used to identify the DoD medical treatment facilities for restructuring, and stated that the DoD based part of its methodology on incomplete and inaccurate information.[94] The report found that civilian health care assessments did not consistently account for provider quality of care and access to an accurate and adequate number of providers near DoD medical treatment facilities, potentially overestimating the purchased care provider network's ability to absorb the patients previously treated at DoD medical treatment facilities. The report also stated that the DoD conducted limited assessments of DoD medical treatment facilities' support to the readiness of military primary care and non-physician medical providers. A DoD OIG audit issued in August 2020 found that 7 of 13 medical treatment facilities (direct care system) or their supporting TRICARE network (purchased care system) did not meet the specialty mental health access to care standard each month, and on average, 53 percent (4,415 of 8,328 per month) of all active duty service members and their families, identified as needing mental health care and referred to the purchased care system, did not receive care and the Military Health System did not know why.[95]

Recently, Congress has expressed concerns about the impact of Military Health System reforms on service members and beneficiaries. The House Committee on Appropriations stated that serious questions remain about the quality and availability of care, and the negative impact on readiness that may be caused by a reduction of military medical providers. The House version of the FY 2021 NDAA would restrict the DoD from restructuring DoD medical treatment facilities or reducing military medical end strength until the DoD provides justification for these initiatives. The House version of the FY 2021 NDAA would have to be adopted by the Senate and signed by the President before it becomes law.

As the DoD implements congressionally mandated and internally driven reforms, it faces the monumental task of establishing joint policies and procedures, transferring administration of the DoD medical treatment facilities to the Defense Health Agency, and gaining efficiencies

[94] Report No. GAO 20-371, "Defense Health Care: Additional Information and Monitoring Needed to Better Position DoD for Restructuring Medical Treatment Facilities," May 29, 2020.

[95] Report No. DODIG-2020-112, "Evaluation of Mental Health Access to Care in the Department of Defense," August 10, 2020.

through personnel realignments, while weighing the risks to force readiness and the health of its beneficiaries.

DEPLOYMENT AND INTEROPERABILITY OF ELECTRONIC HEALTH RECORDS

The DoD deployed a new electronic health records system, MHS GENESIS, in 2017 to help ensure seamless care throughout the life of military members and beneficiaries. Further complicating its implementation is the fact that MHS GENESIS is being jointly developed and operated with the Department of Veterans Affairs. MHS GENESIS is intended to standardize the management and delivery of health care for the 9.5 million beneficiaries in the Military Services and 9.1 million veterans and beneficiaries supported by the Department of Veterans Affairs. MHS GENESIS should provide enhanced, secure technology to access and manage patient health.

The deployment of MHS GENESIS has been challenging. For example, in January 2018, the DoD took an 8-week strategic pause to address approximately 7,000 help desk tickets related to initial deployment of the system, solicit user feedback, address lack of training tools, and begin making system modifications necessary to optimize the system. The Defense Health Agency worked with the contractor to address the identified issues and resumed its roll-out in September 2019. The DoD continues to deploy the system, while addressing implementation issues and known system shortfalls, but recent feedback from military hospitals and clinics has been more positive. The Defense Health Agency plans to field MHS GENESIS to all military hospitals and clinics by 2024.

The DoD OIG and Department of Veterans Affairs OIG began a joint audit in February 2020 to determine the extent to which DoD and Department of Veterans Affairs efforts to implement MHS GENESIS and its supporting architecture will achieve electronic health records interoperability. In April 2020, the Department of Veterans Affairs OIG reported that critical physical and information technology infrastructure upgrades would not be completed until 4 months after deployment.[96] The Department of Veterans Affairs OIG also reported that to meet the Department of Veterans Affairs' deployment dates, clinical staff would have to enact 84 workarounds, which presented a significant patient safety risk.[97]

The DoD will need to work diligently to fix the problems identified during the MHS GENESIS implementation and ensure the system is fully interoperable with the Department of Veterans Affairs. An effective electronic health records system is necessary to prevent safety risks for patients, such as untimely diagnoses, prescription conflicts, ineffective patient outcomes, and patient harm as a result of incomplete patient health information. In addition, a secure electronic health record system is essential to help prevent adversaries from exploiting the personally identifiable information of active duty service members and veterans.

SUBSTANCE ABUSE

Preventing substance abuse and effectively treating military personnel with substance abuse problems continues to be a challenge for the DoD. Substance abuse refers to the harmful or hazardous use of psychoactive substances. While many drugs are illegal, some legal substances can also be dangerous in large quantities, such

[96] Report No. VA OIG 19-08980-95, "Deficiencies in Infrastructure Readiness for Deploying VA's New Electronic Health Record System," April 27, 2020.

[97] Report No. VA OIG 19-09447-136, "Review of Access to Care and Capabilities During VA's Transition to a New Electronic Health Record System at the Mann-Grandstaff VA Medical Center Spokane, Washington," April 27, 2020.

as alcohol or prescription medication if not taken as prescribed. For example, opioid use disorders among military personnel often begin with an opioid pain prescription following an injury during deployment. However, due to the addictive nature of opioids, particularly coupled with mental health struggles experienced by some military personnel, regular or extended use of opioids can lead to addiction.

While illicit drug use among active duty personnel is relatively low, rates of binge drinking are high compared to the general population. Alcohol use disorders are the most prevalent form of substance use disorders among military personnel.[98] In 2019, the prevalence of alcohol-related disorders was six times higher than that of all other substance use disorders combined. According to the Psychological Health Center of Excellence, in 2019, 21,975 active duty service members had an alcohol-related disorder, compared to 3,464 active duty service members who had a substance-related disorder. 2019 also saw more than 422,500 outpatient visits associated with alcohol-related care in the Military Health System.[99] Figure 2 shows the number of active duty service members that had alcohol and substance-related disorders from 2005 through 2019.

Active duty service members' willingness to seek and access treatment for substance abuse remains a challenge for the DoD. The DoD has personnel security reporting requirements, zero-tolerance policies, and in certain cases, providers are required to disclose the identities of those under their care. These same policies and reporting requirements may potentially discourage those who need treatment from seeking it. For example, according to an October 2019 report by the National Institute on Drug Abuse within the Department of Health and Human Services, half of military personnel have reported that they believe seeking help for mental health issues, such as substance abuse, would negatively affect their military career.[100]

In 2016, TRICARE expanded its treatment services to improve access to substance use disorder treatment for all TRICARE beneficiaries. The Defense Health Agency's Evaluation of the TRICARE Program Fiscal Year 2019 Report to Congress stated that visits to the mental health and substance use disorder intensive outpatient program quadrupled from FY 2016 to FY 2017. Preventing substance abuse and effectively treating active duty personnel with substance abuse problems continues to be a challenge for the DoD.

SUICIDE PREVENTION

Suicide prevention has been an ongoing top priority for Congress and the DoD; nevertheless, suicide rates within the DoD continue to climb.[101] DoD leadership continues to develop strategies and employ efforts at all echelons to raise awareness of and prevent suicide. The Vice Chairman of the Joint Chiefs of Staff said in September 2020, "Regardless of the uniform we wear, we are not immune from life's challenges, including thoughts of suicide," and also stressed, "Ending suicide in our ranks is a top priority."

In 2015, Congress directed the Defense Suicide Prevention Office to collaboratively develop a Defense Strategy for Suicide Prevention that aligns with the 13 Goals and 60 Objectives of the National Strategy for Suicide Prevention and with the Military Service suicide prevention

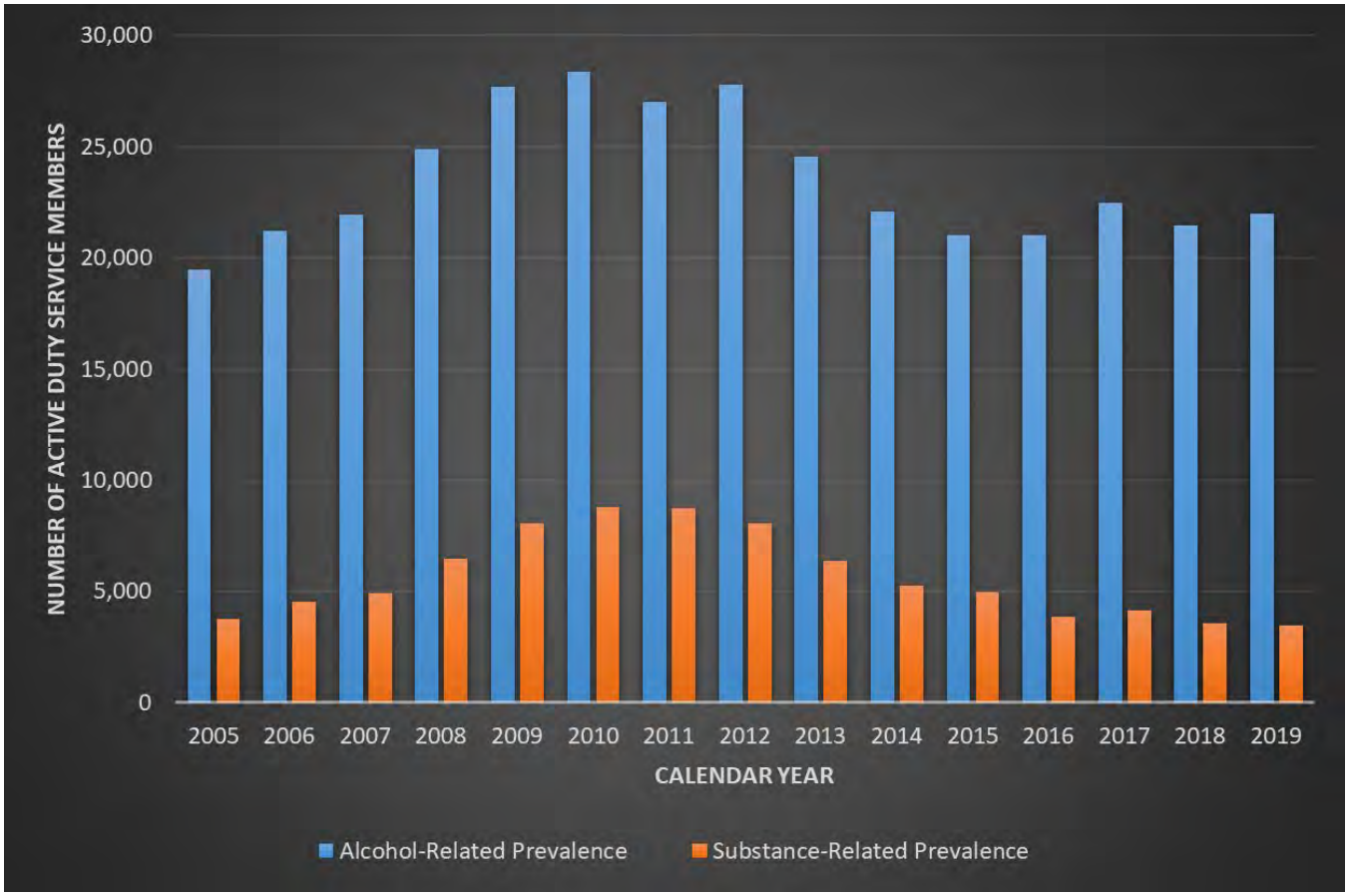
98 National Institute on Drug Abuse, "Substance Use and Military Life," October 2019.

99 Psychological Health Center of Excellence (PHCoE), "Prevalence of Mental Health Conditions Among Active Duty Service Members From 2005-2019."

100 National Institute on Drug Abuse, "Substance Use and Military Life," October 2019.

101 DoD, "Department of Defense Suicide Event Record 2018."

Figure 2. Active Duty Service Member Alcohol-Related Prevalence and Substance-Related Prevalence



Source: DoD OIG-generated from data provided by the Psychological Health Center of Excellence.

programs. The Defense Suicide Prevention Office issued guidance in November 2017 that outlined processes for planning, directing, guiding, and resourcing to effectively develop and integrate the Suicide Prevention Program within the DoD. However, the lack of oversight of the Military Service implementation and limited use of evidence-based practices led to the FY 2020 NDAA requirement for the Government Accountability Office to comprehensively evaluate DoD suicide prevention efforts. In September 2020, the Defense Suicide Prevention Office issued an update to its 2017 guidance. Nevertheless, the Defense Strategy for Suicide Prevention and the DoD guidance do not include medical prevention, intervention and post-intervention practices, and only briefly mention using evidence-based practices and following existing guidance published by the Assistant Secretary of Defense for Health Affairs. The lack of a well-coordinated approach has led to misaligned terms and definitions, gaps in data collection and reporting concerns, and confusion over who is ultimately responsible for the suicide prevention planning and implementation at the Military Service levels and below.

By comparison, the 2013 Suicide Risk Clinical Practice Guideline for the Assessment and Management of Patients at Risk for Suicide was updated in 2019. The guidelines include more recent objective, evidence-based information on the assessment and management of suicide risk. This information, however, has not been integrated into the Defense Strategy for Suicide Prevention or the DoD guidance published by the

Defense Suicide Prevention Office. The clinical and non-clinical strategies for suicide prevention are not coordinated and are not under one overarching authority for implementation.

The 2018 DoD Suicide Event Report, published in April 2020, stated that there was evidence of an increase in the suicide mortality rate from 2011 through 2018 for the active components in each of the Military Services. In March 2020, the Government Accountability Office began evaluating current programs and activities of the DoD and the Armed Forces for the prevention of suicide among members of the Armed Forces and their families. Suicides among service members continue to be a major challenge for the DoD, and prevention efforts are key to caring for those personnel as evidenced by congressional mandates and by Government Accountability Office and DoD OIG reports and recommendations.

IMPACT OF ENVIRONMENTAL HAZARDS ON DOD PERSONNEL

While environmental hazards, contaminants, and pollution may not always pose an immediate threat to DoD operations, they may become important drivers for DoD missions, programs, enterprise-wide resources, and liabilities in the future.

Despite Federal regulations, environmental hazards—such as lead-based paint, asbestos-containing material, and contaminated drinking water—continue to be well-known threats to military personnel and their families. Some emerging contaminants and pollutants, however, are not regulated or are loosely regulated. The DoD defines emerging contaminants as "Chemicals relevant to the DoD that are characterized by a perceived or real threat to human health or the environment and that have new or changing toxicity values or new or changing human health or environmental regulatory standards. Changes may be due to new science discoveries, detection capabilities, or exposure pathways."[102] The changing nature of science and regulation surrounding emerging contaminants and pollutants creates challenges for the DoD as officials work to mitigate potential risks.

Emerging contaminants include perfluoroalkyl and polyfluoroalkyl substances, also known as PFAS or "forever chemicals." PFAS are found in everyday consumer items, from nonstick cookware to water-resistant clothing. The DoD's primary use of PFAS started in the 1970s, with the introduction of fire suppressant foam, which contained certain PFAS, used to fight fuel-based fires.[103] Although agencies such as the DoD and the U.S. Environmental Protection Agency have been participating in studies and taking actions to characterize, identify, and develop methods to test for and dispose of PFAS since the early 2000s, media attention in 2018 and 2019 led to congressional hearings and the formation of the DoD PFAS Task Force in 2019. As of June 30, 2020, the DoD had identified 676 DoD installations where PFAS-containing fire suppressant foam may have been used or released.

The DoD is facing a variety of challenges to address PFAS concerns, including mitigating the release of fire suppressant foam containing PFAS; researching and developing a PFAS-free fire suppressant to fight fuel-based fires; identifying and mitigating exposure to other potential DoD sources of PFAS; monitoring and communicating information on the health effects of human exposure to PFAS; establishing policies and

[102] DoD Instruction 4715.18, "Emerging Chemicals (ECS) of Environmental Concern," September 4, 2019.

[103] The foam is called aqueous film-forming foam.

A U.S. Navy Hospital Corpsman, assigned to Expeditionary Medical Facility Camp Pendleton, California, looks through a microscope in the lab during a training exercise at Naval Base Guam. (U.S. Navy photo)

collecting data to track PFAS cleanup progress and costs; and supporting research and development efforts for all of these activities.

Another environmental concern the DoD is addressing is the effects of open-air burn pits. Open-air burn pits were commonly used in Iraq and Afghanistan to dispose of waste such as chemicals, paint, medical and human waste, munitions and other unexploded ordnance, and petroleum and lubricant products. In November 2018, the DoD established a policy that the use of open-air burn pits would only be allowed in short-term contingency operations where no feasible alternative exists.[104] Open-air burn pits create more air pollution than conventional solid waste management methods, such as incinerators. According to the Department of Veterans Affairs, research does not currently show evidence of long-term health problems for people exposed to open-air burn pits, but it does recognize that veterans who were near the smoke or exposed for longer periods may be at greater health risk. However, according to a 2019 McClatchy article, instances of some forms of cancer for veteran beneficiaries within the Department of Veterans Affairs have risen significantly during the Iraq and Afghanistan wars. For example, according to McClatchy, the urinary cancer rate has increased by 61 percent and liver and pancreatic cancer rates have risen by 96 percent for veterans from 2000 to 2018. According to the article, many veterans associate their cancer with the toxic chemicals and burn pits they were exposed to while serving in the military.

In a 2019 report to Congress, the DoD stated that it is sharing information with the Department of Veterans Affairs' Airborne Hazards and Open Burn Pit Registry, in which eligible veterans and service members can document their exposures and report health concerns through an online questionnaire. The DoD is also conducting joint studies with

[104] DoD Instruction 4715.19, "Use of Open-Air Burn Pits in Contingency Operations," November 13, 2018.

the Department of Veterans Affairs to identify service members' exposures during deployments to Iraq and Afghanistan and track any long-term health effects.

The DoD initially issued guidance in 2009 about the identification, assessment, and management of emerging chemicals of environmental concern relevant to the DoD.[105] Additionally, the DoD issued guidance in 2017 to establish procedures for assessing significant long-term health risks from past environmental exposures while living or working on military installations.[106] Service members, their families, and civilians may be exposed to environmental hazards as a result of many factors, such as lack of regulations or poor risk management and prevention. The news media often report on DoD personnel exposed to environmental hazards, including both regulated hazards and emerging contaminants, as a result of both occupational and non-occupational exposures. Identifying and remediating unsafe conditions and treating any resultant health issues are challenges for the DoD.

HEALTH AND SAFETY MANAGEMENT OF MILITARY FAMILY HOUSING

Ensuring military family housing is free from health and safety hazards is a key element of the DoD's commitment to protect and provide for its military personnel and their families. The DoD's policy is to "Ensure that eligible personnel and their families have access to affordable, quality housing facilities and services consistent with grade and dependent status and generally reflecting contemporary community living standards."[107] The DoD offers housing for service members and their families as a benefit and when housing is not available in the local community. Safe housing is vital for military families because it gives service members peace of mind regarding their families, especially when deployed. Knowing that their families have a well-maintained, structurally safe home that does not pose health, safety, or fire hazards enables them to better focus on their mission.

Since 2015, several Government Accountability Office, DoD OIG, and Military Department oversight reports have highlighted that the DoD needs to improve its oversight of military family housing, especially privatized military family housing.[108] The concerns about health and safety hazards in military family housing, voiced by media and congressional testimony, reached a peak during 2018 and 2019, resulting in extensive requirements for military housing reform in the FY 2020 NDAA. Government Accountability Office and DoD OIG reports published in 2020 showed

[105] DoD Instruction 4715.18, "Emerging Chemicals (ECS) of Environmental Concern," September 4, 2019.

[106] DoD Instruction 6055.20, "Assessment of Significant Long-Term Health Risks from Past Environmental Exposures on Military Installations," June 6, 2017.

[107] DoD Manual 4165.63, "DoD Housing Management," October 28, 2010, incorporating change 2, August 31, 2018.

[108] Report No. GAO-19-73, "Defense Real Property: DoD Needs to Take Additional Actions to Improve Management of Its Inventory Data," November 13, 2018.

Report No. GAO-18-218, "Military Housing Privatization: DoD Should Take Steps to Improve Monitoring, Reporting, and Risk Assessment," March 13, 2018.

Report No. DODIG-2017-118, "Followup Evaluation on DoD Office of Inspector General Report No. DODIG- 2014-121, 'Military Housing Inspection-Japan,'" September 30, 2014," September 14, 2017.

Report No. DODIG-2017-104, "Followup on DoD OIG Report No. DODIG-2015-013, 'Military Housing Inspections – Republic of Korea, October 28, 2014,'" July 20, 2017.

Report No. DODIG-2017-004, "Summary Report – Inspections of DoD Facilities and Military Housing and Audits of Base Operations and Support Services Contracts," October 14, 2016.

Report No. DODIG-2016-139, "Military Housing Inspection – Camp Buehring, Kuwait," September 30, 2016.

Report No. DODIG-2015-181, "Continental United States Military Housing Inspections – Southeast," September 24, 2015.

Report No. DODIG-2015-162, "Continental United States Military Housing Inspections – National Capital Region," August 31, 2015.

Report No. DODIG-2015-013, "Military Housing Inspections – Republic of Korea," October 28, 2014.

that the DoD still has considerable challenges to reforming the management of both privatized and Government-owned, Government-controlled military family housing.

In March 2020, the Government Accountability Office found that the DoD did not use reliable or consistent data to report on the condition of privatized housing and that military housing offices were not effectively communicating their role as a resource for service members experiencing challenges.[109] In April 2020, the DoD OIG reported systemic deficiencies in the management of health and safety hazards in Government-owned, Government-controlled military family housing, such as lead-based paint, asbestos-containing material, and radon. The report also found that the Military Services' oversight inspection and audit policies, procedures, and checklists were not designed to address the management of health and safety hazards in Government-owned, Government-controlled military family housing.[110]

To reform military housing, the FY 2020 NDAA requires the DoD to clarify contract management and establish the Military Housing Privatization Initiative Bill of Rights; evaluate the extent to which shortages in the number of civilian personnel contribute to problems regarding the management of privatized military housing; and establish a dedicated health and safety hazard management tool and process to identify and address hazards in military family housing. As of September 2020, the DoD had implemented 14 of the 18 tenets of the Military Housing Privatization Initiative Bill of Rights. The DoD is working to implement the four remaining rights related to leases, dispute resolution, and availability of maintenance histories of housing.

To address concerns about military housing, the FY 2020 NDAA also mandated that the DoD OIG conduct three evaluations from FY 2020 to FY 2022 to report on the DoD's oversight of military family housing. The first evaluation began in March 2020 and focuses on privatized military family housing contract management.[111] The second and third evaluations will focus on the management of health and safety in privatized military family housing. The evaluations should help clarify issues related to military family housing and provide actionable findings and recommendations for the DoD to address this challenge.

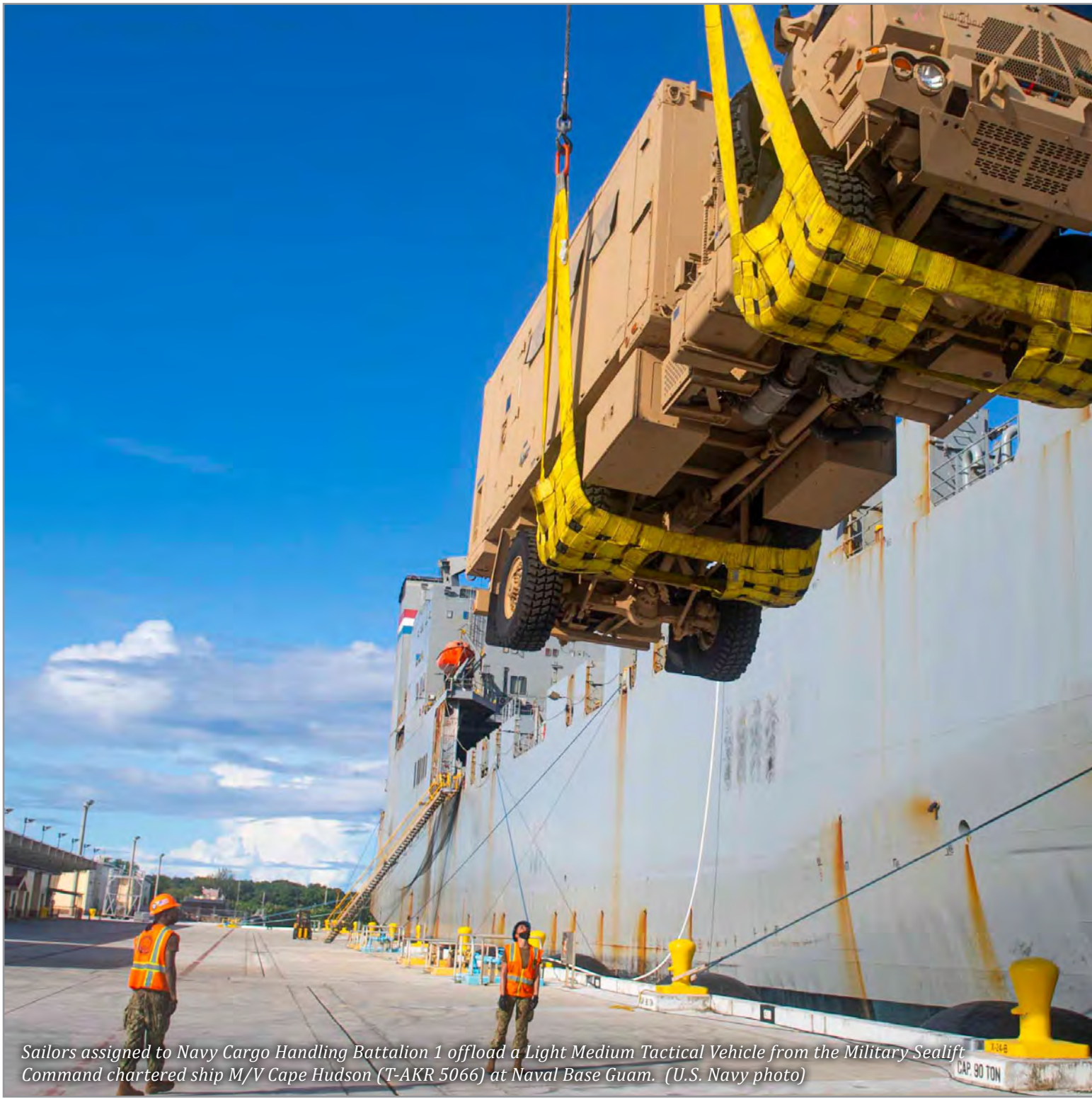
CONCLUSION

To fulfill the DoD's commitment to its personnel, the DoD must continue providing service members, retirees, and their families with access to high-quality health care, substance abuse and suicide prevention programs, and adequate housing. The DoD must continue to mitigate the impact of environmental hazards and exposure to chemicals used by the DoD on the health of its personnel and their families.

[109] Report No. GAO-20-281, "Military Housing: DoD Needs to Strengthen Oversight and Clarify Its Role in the Management of Privatized Housing," March 26, 2020.

[110] Report No. DODIG-2020-082, "Evaluation of the DoD's Management of Health and Safety Hazards in Government-Owned and Government-Controlled Military Family Housing," April 20, 2020.

[111] Project No. D2020-DEV0PA-0096.000, "Evaluation of Department of Defense Oversight of Privatized Military Housing Contracts," March 2, 2020.



Sailors assigned to Navy Cargo Handling Battalion 1 offload a Light Medium Tactical Vehicle from the Military Sealift Command chartered ship M/V Cape Hudson (T-AKR 5066) at Naval Base Guam. (U.S. Navy photo)

Challenge 8. Strengthening and Securing the DoD Supply Chain and Defense Industrial Base

INTRODUCTION AND OVERVIEW

A resilient and robust supply chain is critical to ensuring that the DoD has the parts and equipment it needs to maintain readiness. At the heart of the DoD's supply chain is the extremely complex Defense Industrial Base, encompassing over 300,000 companies supporting the DoD, who provide the DoD with the tools, capabilities, and resources needed to protect and secure the Nation. The Defense Industrial Base includes domestic entities and foreign entities located around the world, and is susceptible to foreign influence and cyber attacks. In one essential sector, rare earth elements, the DoD is overly reliant on foreign sources due to the lack of U.S. companies that mine and process rare earth elements. Every step in the supply chain is important, beginning with identifying a need; continuing through manufacturing, purchasing, delivery, distribution, maintenance, repair, and sustainment; and ending with disposition. Failure to reduce barriers throughout the entire process may add unnecessary delays getting vital parts to service members. Without a stable and resilient supply chain and industrial base, DoD operations may be at risk.

Strengthening and securing the supply chain and the Defense Industrial Base remain a top challenge for the DoD. To strengthen the supply chain, the DoD should encourage innovation and attract new trusted suppliers. This can be accomplished by streamlining the acquisition process; considering technical data rights at the beginning of the acquisition process; and using emerging technologies, such as artificial intelligence and advanced manufacturing, to improve efficiencies and fill gaps in the supply chain. Finally, securing the Defense Industrial Base from foreign influence, bad actors, and cyber attack remains a critical challenge for the DoD.

STRENGTHENING THE SUPPLY CHAIN

The 2018 National Defense Strategy states that innovating and reforming the DoD's approach to doing business are key to sustaining U.S. influence and protecting the industrial base. U.S.-based companies may decide not to compete to be a part of the DoD supply chain because of cumbersome acquisition and contracting practices or the lack of contract stability due to DoD budget uncertainty. The DoD's lengthy procurement process

and limited suppliers contribute to higher costs and delays in maintaining DoD systems and equipment.

REDUCING BARRIERS THROUGH STREAMLINING THE ACQUISITION PROCESS

Congress and the DoD have sought to reform the DoD acquisition process, long considered to be cumbersome and lengthy, to streamline the development and fielding of technologies to get needed capabilities in the hands of service members. A 2017 Government Accountability Office report stated that innovative companies may choose not to do business with the DoD due to the complexity of the DoD's processes, uncertain Federal budget environment, intellectual property concerns, and long contracting timelines.[112] Since that time, the DoD has taken steps to streamline the acquisition process to attract new suppliers.

Section 804 of the National Defense Authorization Act (NDAA) for FY 2016 required the DoD to reform its acquisition process to field capabilities faster. The reforms included an alternative acquisition process, known as rapid acquisition, which requires DoD Components to complete programs by fielding prototypes or systems with proven technologies within 5 years of beginning the acquisition.

Rapid acquisition, however, is not without its challenges. In the DoD's urgency to rapidly develop prototypes, DoD Components may have selected technologies for rapid prototyping that will never be fully developed or will not address capability gaps. Additionally, due to budgetary adjustments and changing priorities, DoD Components may not be able to afford to transition successful prototyping efforts into acquisition programs. As of April 2020, DoD Components had 71 ongoing rapid acquisition programs valued at about $59.4 billion. Some prototype efforts may never come to fruition, resulting in sunk costs to those terminated programs. Therefore, it is important that DoD Components use best practices to select technologies for rapid prototyping that prioritize warfighter needs and long-term affordability. The DoD OIG has an ongoing audit to determine whether the DoD Component acquisition officials managed programs, in accordance with DoD guidance, for the middle-tier acquisition approaches, using either rapid prototyping or rapid fielding, to deliver a capability within 2 to 5 years of the development of an approved requirement. Rapid acquisition authorities provide the DoD with innovative ways to quickly field new capabilities, but also present new challenges the DoD must consider, including how to ensure appropriate oversight of the rapid acquisition authority, and in particular ensuring that the DoD is making informed decisions and meeting performance metrics.[113]

In January 2020, the DoD published a new adaptive acquisition framework that provides greater flexibility within the acquisition process, and aims to improve the speed of acquisitions by reducing bureaucratic roadblocks. The framework outlines an acquisition strategy made up of six acquisition pathways, each tailored to the unique characteristics and risk profiles of the acquired capability.[114] The framework gives more authority to program managers and decision makers at the beginning of the acquisition process, while assigning

[112] Report No. GAO-17-644, "DoD Is Taking Steps to Address Challenges Faced by Certain Companies," July 20, 2017.

[113] Report No. GAO-19-439, "DoD Acquisition Reform: Leadership Attention Needed to Effectively Implement Changes to Acquisition Oversight," June 2019.

[114] DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020.

primary program authority to the Offices of the Under Secretaries of Defense for Acquisition and Sustainment and for Research and Engineering. Implementing the framework should help improve transactions between the DoD and the Defense Industrial Base, avoid delays at the end of the acquisition, and increase the speed of critical Defense acquisitions.

OBTAINING THE TECHNICAL DATA RIGHTS NEEDED TO SUSTAIN DOD WEAPON SYSTEMS

The DoD's ability to plan preventative maintenance, properly repair items, and perform sustainment activities is critical to ensuring system and equipment readiness. The DoD should consider technical data rights during the acquisition process because data rights issues impact supply chain availability and the DoD's ability to organically (with DoD personnel in DoD facilities) or competitively sustain items. Many suppliers often refuse to deliver certain technical data citing intellectual property concerns, offer data at an unreasonable price, or place restrictions on the Government's rights to use technical data. The DoD must ensure it is negotiating early in the acquisition process for the appropriate licenses to ensure the technical data is part of the acquisition, fielding, or sustainment strategy.

For example, the DoD OIG found that the Navy and Defense Logistics Agency both faced challenges in obtaining technical data needed to fill back orders for critical spare parts on the F/A-18 Super Hornet, in part because of the high cost of obtaining the technical data rights.[115] Figure 3 shows a communication antenna from the F/A-18 Super Hornet, a critical part that was back-ordered because of a lack of technical data rights. According to the Defense Logistics Agency, the only contractor capable of making the antenna had long lead times and capacity limitations, which caused the backorders. If the DoD had had the technical data rights for the antenna, it could have found alternative sources to produce the antenna.

Figure 3. Communication Antenna for the Super Hornet

Source: The Defense Logistic Agency.

Data rights issues impact parts availability and the DoD's ability to organically or competitively sustain items. For example, the DoD and Lockheed Martin have disagreed on intellectual property and data rights for the F-35 aircraft. In November 2019, the Government Accountability Office testified before a House Armed Services Subcommittee that the DoD lacked the technical data from Lockheed Martin needed to fully understand the technical characteristics of the F-35 aircraft and enable potential competition of future sustainment contracts.[116]

[115] Report No. DODIG-2020-030, "Audit of Navy and Defense Logistics Agency Spare Parts for F/A-18 E/F Super Hornets," November 19, 2019.

[116] Report No. GAO 20-234T, Testimony Before the Subcommittees on Readiness and Tactical Air and Land Forces, Committee on Armed Services, House of Representatives, "F-35 Aircraft Sustainment: DoD Faces Challenges in Sustaining a Growing Fleet," November 13, 2019.

To address the issue of data rights, the Office of the Under Secretary of Defense for Acquisition and Sustainment issued policy on how the DoD should acquire and license intellectual property for its weapons and information systems, and the operations, maintenance, sustainment, and cost of the systems.[117] The policy established an intellectual property cadre of experts within the Office of the Under Secretary to bring more rigor and consistency to how the DoD handles intellectual property in its contract negotiations with vendors. The new cadre is charged with the development and update of the DoD's policies on data rights and working on concerns related to intellectual property theft. Properly planning for system sustainment, including intellectual property rights, is critical in ensuring the DoD meets national security objectives.

IMPROVING SUPPLY CHAIN EFFICIENCIES THROUGH ARTIFICIAL INTELLIGENCE

The DoD has had longstanding challenges in tracking inventory, distributing available spare parts, and forecasting appropriate stock levels to maintain equipment and systems.[118] To address these challenges, the DoD is leveraging artificial intelligence (AI) to improve materiel management and decision making. AI refers to the ability of machines to perform tasks that normally require human intelligence, such as recognizing patterns. AI also refers to the software that controls autonomous physical systems.

The DoD uses AI in supply chain management to predict the failure of critical parts, automate diagnostics, and plan maintenance based on historical data and equipment condition. AI can also improve the management of spare parts and optimize inventory levels. For example, the Air Force has successfully implemented predictive maintenance techniques in the E-3 Sentry (AWACS), C-5 Galaxy, and the F-16 Fighting Falcon aircraft. According to the Defense Innovation Unit 2019 Annual Report, the Air Force has demonstrated the potential for a 3- to 6-percent improvement in mission capability, up to a 35-percent reduction of base-level occurrences of aircraft sitting on the ground awaiting parts, and up to a 40-percent reduction in unscheduled maintenance events. The DoD OIG has projects planned on predictive maintenance, including one that will focus on sustaining weapon systems and another on the Bradley fighting vehicle and the M88 armored recovery vehicle.

FILLING GAPS IN THE SUPPLY CHAIN THROUGH ADVANCED MANUFACTURING

Advanced manufacturing is the use of innovative technology to improve products and manufacturing processes. It includes, but is not limited to, additive manufacturing (also known as three-dimensional printing), robotics, and the use of advanced composite materials, such as carbon fiber or polymers, to improve a product's performance.

Additive manufacturing creates an object by adding layers of material from three-dimensional data, unlike traditional, or subtractive, manufacturing processes where the product is created by cutting away material from a larger piece. By using additive manufacturing, the DoD has been able to manufacture some parts to supplement the supply chain when the part is unavailable in a timely manner or is obsolete. According to a 2019 DoD OIG report on additive manufacturing, at least 81 Military Service depots, maintenance facilities, and field

[117] DoD Instruction 5010.44, "Intellectual Property Acquisition and Licensing," October 16, 2019.

[118] GAO High Risk List 2019.

locations were using additive manufacturing to produce thousands of parts and tools, thereby decreasing maintenance times, reducing the impact of obsolete parts no longer available through traditional manufacturing sources, and improving existing parts.[119]

To further develop advanced manufacturing capabilities, the Army established the Center of Excellence for Advanced Manufacturing at Rock Island Arsenal, Illinois. The Center serves as a central location to develop best practices and operationalize additive and advanced manufacturing across the Army. Army Directive 2019-29, "Enabling Readiness and Modernization Through Advanced Manufacturing," states that advanced manufacturing will fundamentally change the way the Army designs, delivers, produces, and sustains materiel capabilities. The DoD must continue incorporating advanced manufacturing throughout a system's life cycle, beginning with design and development and continuing throughout sustainment.

The 2019 DoD OIG report on additive manufacturing found that the Army and Marine Corps developed transportable facilities to allow soldiers and marines to manufacture parts in a deployed environment.[120] This type of innovation allows for greater flexibility when parts or equipment break down and there is not a sufficient supply or the time to wait for resupply. Figure 4 shows a Marine Corps Expeditionary Fabrication Facility.

The DoD can use advanced manufacturing to address sustainment and readiness challenges related to parts obsolescence, diminishing sources of supply, or replacing parts within assemblies that the DoD would normally have to purchase whole. For example, the same 2019 DoD OIG report highlighted that an F-35 landing gear door bump stop must be purchased as part of the traditionally produced landing gear assembly for $70,000; however, the Navy used additive manufacturing to produce just the bump stop for only $0.75. With a continued focus on advanced manufacturing, the DoD can mitigate supply chain risk and achieve savings while improving materiel readiness.

Figure 4. Marine Corps Expeditionary Fabrication Facility

Source: The Marine Corps.

SECURING THE DEFENSE INDUSTRIAL BASE

The DoD supply chain and Defense Industrial Base may experience instability and security concerns when only a few sources can provide needed supplies, or the DoD is competing with other countries for the same resources. The United States relies on foreign sources of supply to provide rare earth elements used in defense systems and technology hardware and software. Additionally, physical security and cybersecurity are critical to protecting the DoD supply chain. The Defense Logistics Agency supplies 86 percent of the military's spare parts and nearly 100 percent of fuel and supplies, and developed a comprehensive supply chain security strategy to mitigate the physical and cybersecurity risk to the

[119] Report No. DODIG-2020-003, "Audit of the DoD's Use of Additive Manufacturing for Sustainment Parts," October 21, 2019.

[120] Ibid.

supply chain. Furthermore, the DoD relies on contractors for significant contributions to the supply chain, leading to the need to secure contractor networks that contain DoD data. The Office of the Under Secretary of Defense for Acquisition and Sustainment has developed the Cybersecurity Maturity Model Certification Program to require third-party companies to certify that DoD contractors maintain the appropriate levels of cybersecurity, ensure basic cyber hygiene, and protect Controlled Unclassified Information. The DoD's cybersecurity challenges are discussed further in Management Challenge 5, "Enhancing Cyberspace Operations and Capabilities, and Securing the DoD's Information Systems, Networks, and Data."

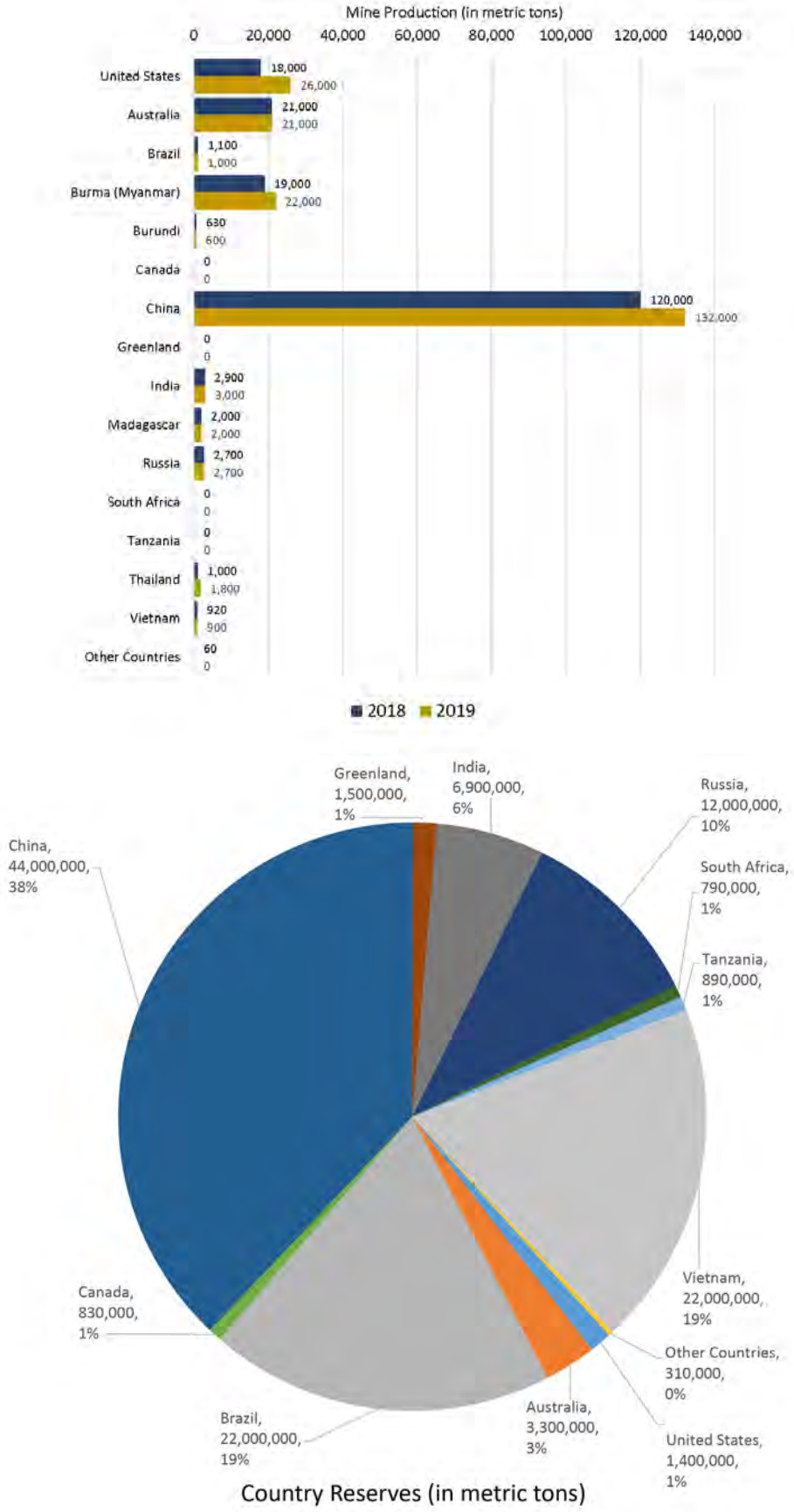
REDUCING DEPENDENCE ON FOREIGN SOURCES FOR RARE EARTH ELEMENTS

Rare earth elements are critical elements valuable for their unique characteristics, such as magnetic properties, corrosion resistance, luminescence, and electrical conductivity. They are used across many major weapon systems, including lasers, radar, sonar, night vision systems, missile guidance, jet engines, and even alloys for armored vehicles. Despite their name, according to a January 2020 article published by the Army War College, most rare earth elements are relatively abundant. The process of mining rare earths and transforming them into usable materials is, however, expensive and damaging to the environment. The high cost and harmful effects of rare earth mining and processing forced U.S. companies in the late 1990s to reduce or close their operations.

According to the U.S. Geological Survey's 2020 report on rare earth elements, from 2015 to 2018 the United States imported 80 percent of its rare earth elements from China, which presents a risk to U.S. national security and Defense Industrial Base. This risk was highlighted in May 2019, when the Chinese state media suggested cutting off rare earth element supplies to the United States in response to the U.S. Department of the Treasury naming Huawei, the Chinese global communications and technology company, a national security threat. Figure 5 shows the metric tons of rare earth elements produced by country in 2018 and 2019 and demonstrates China's dominance in rare earth element mine production and reserves.

The Administration and Congress have recognized the need to reduce dependency on China for rare earth elements. In the last year, the DoD has awarded two contracts to Australian and U.S. companies to create rare earth element separation facilities within the United States. The DoD is also seeking to develop equipment and processes to mine rare earth elements. For example, in July 2020, the DoD announced a $28.8 million agreement with a mining company to develop a domestic source for a type of rare earth magnet—neodymium iron boron. This rare earth element magnet is a key component in some DoD systems, allowing for miniaturization and higher performance of guidance, propulsion, and power systems. The Senate Armed Services Committee report accompanying the FY 2021 NDAA expressed support for the DoD's efforts to identify and acquire secure sources of rare earth elements. Additionally, in September 2020, the President issued an Executive order directing the U.S. Government, including the DoD, to investigate the United States' reliance on foreign adversaries for rare earth elements and enhance its mining and processing capability.

Figure 5. Rare Earth Element Production by Country in 2018 and 2019



Source: The DoD OIG and U.S. Geological Survey.

PROTECTING AGAINST FOREIGN INFLUENCE IN THE SUPPLY CHAIN

The DoD must continue to be aware of foreign intrusion and influence on the Defense Industrial Base and ensure adversaries do not control companies and resources that provide the DoD with critical supplies. Originally established in 1975, the Committee on Foreign Investment in the United States is an interagency committee authorized to review certain transactions involving foreign investment in the United States and certain real estate transactions by foreign persons to determine the effect of the transactions on national security. Congress recognized the continuing risk of foreign influence on U.S. businesses and expanded the authorities of the Committee in the Foreign Investment Risk Review Modernization Act of 2018. The Act expanded the Committee's authority to include more discrete transactions, such as real estate purchases or membership on boards of directors. The Committee can require the parties involved to meet conditions or refer the decision to the President, who can suspend, prohibit, or deny the foreign investment.

In an April 2020 press briefing, the Under Secretary of Defense for Acquisition and Sustainment stated that the United States and countries in Europe have seen instances in which shell companies tried to acquire businesses and the owner of the shell companies ended up being an adversary. Because of this action by U.S. adversaries, the Under Secretary stated that the DoD wanted to further strengthen the Committee's authorities to ensure that the DoD has the necessary statutory tools to intervene.

PROTECTING AND DEFENDING THE DEFENSE LOGISTICS AGENCY SUPPLY CHAIN

The Defense Logistics Agency manages nine supply chains of about 5 million items that support the DoD and other Federal agencies. Processing more than $42 billion in goods and services annually for the U.S. Government, the Defense Logistics Agency developed and began to implement a Supply Chain Security Strategy in FY 2018.[121] The strategy takes a holistic approach to supply chain security and outlines a comprehensive framework to prevent, detect, protect, and defend against threats; build supply chain security into its business enterprise infrastructure; ensure data integrity; partner with reputable vendors; and strengthen resilience across the supply chain. Two areas that have already been implemented are controls to identify risky suppliers, such as bad actors or those with indicators of fraud or noncompliance with rules and regulations, and enhancing the protection of DoD data stored on Defense Logistics Agency systems.

The Defense Logistics Agency has improved its vendor vetting process within its acquisition systems and increased access controls for vendors trying to access export-controlled data. The process has improved controls over technical data by developing the capability to block foreign internet protocol (IP) addresses from accessing the information, and enhanced the capability to identify potential fraud for one of its purchasing systems. The system can identify and then block vendors that flood the system with offers. The Defense Logistics Agency is also refining and implementing tools and analytics platforms to help identify vendor

[121] Defense Logistics Agency, "Supply Chain Security Strategy," Appendix 1 to the Defense Logistics Agency's 2018-2026 Strategic Plan.

relationships and enhance the DoD's ability to identify, report, and prosecute potential counterfeit activity. The DoD must continue to be proactive in identifying risky suppliers because bad actors will continue to adapt.

ENSURING CYBERSECURITY IN DOD ACQUISITIONS

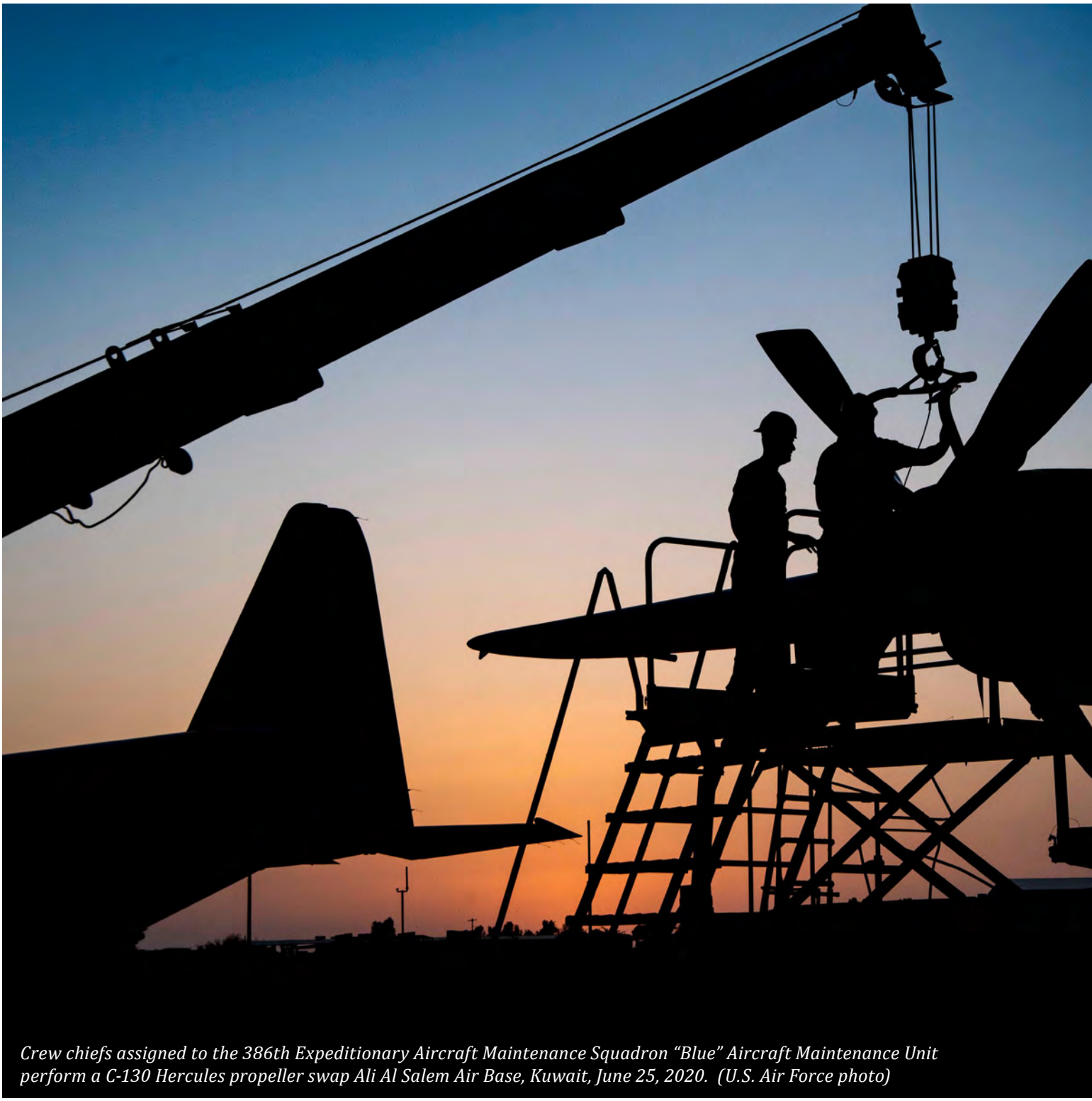
Intellectual property theft from the Defense Industrial Base threatens to reshape the overall distribution of military power between the United States and its adversaries. The Defense Industrial Base, with over 300,000 companies supporting the DoD, is an attractive target for cyber attacks by adversaries and non-state actors. The theft of intellectual property and unclassified data also presents national security risks.

To protect DoD data on non-DoD systems from cyber attacks, the Office of the Under Secretary of Defense for Acquisition and Sustainment developed the Cybersecurity Maturity Model Certification Program. The program seeks to provide assurance to the DoD that its information is protected on non-DoD systems at a level commensurate with the risk of protecting Controlled Unclassified Information, accounting for information flow down to its subcontractors in a multi-tier supply chain. The program also requires a third party to review the controls, processes, and systems of a potential contractor and then certify the contractor's system as level 1, the most basic protection, through level 5, the most sophisticated protection.

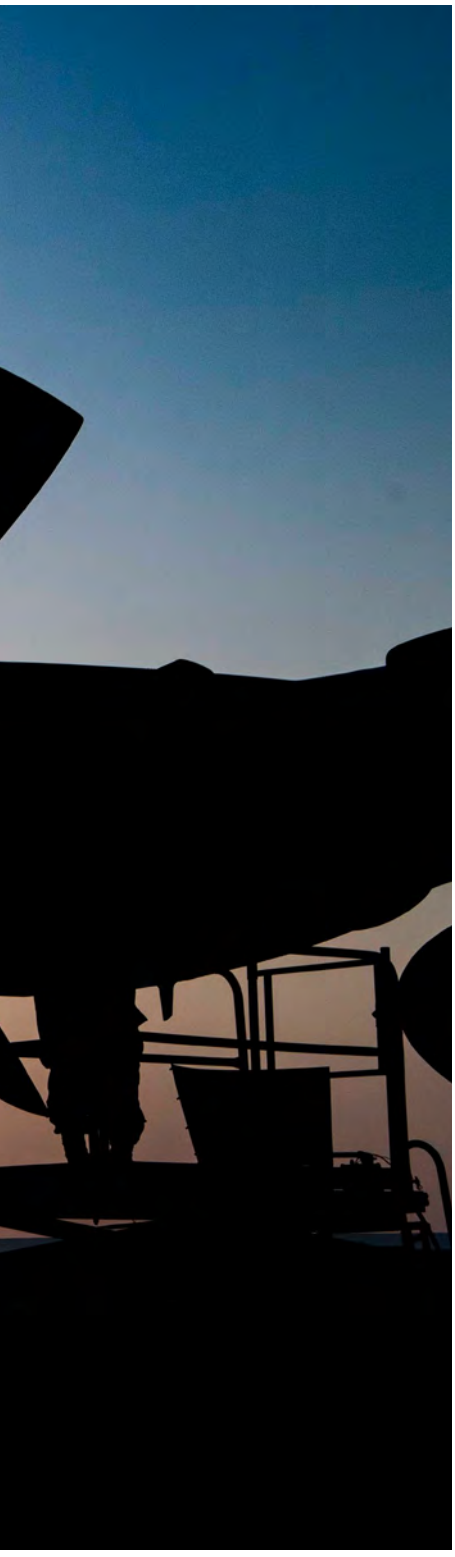
According to a July 2020 National Defense Magazine article, the Chief Information Security Officer in the Office of the Under Secretary of Defense for Acquisition and Sustainment stated that the DoD estimates that 7,500 companies will have a Cybersecurity Maturity Model Certificate in 2021. The DoD OIG plans to perform oversight of the certificate program after the DoD fully implements it. The DoD OIG also plans to audit the security of DoD information stored on the networks and systems of contractors, academic institutions, and research institutions. The DoD's continued investment in enhanced tools to identify and defeat threats will help the DoD strengthen and secure the supply chain and the Defense Industrial Base.

CONCLUSION

The supply chain and Defense Industrial Base are essential to the DoD's ability to perform its mission. The DoD must ensure it uses the rapid acquisition authorities to obtain needed supplies, while also securing technical data rights and employing new technologies to sustain and maintain DoD weapon systems. Although the DoD is making strides to improve its procurement practices, it will continue to face challenges until it can stabilize the Defense Industrial Base, increase trusted sources of supply, and secure those sources of supply from potential threats. Delivering the necessary equipment and parts at the right place and time to the service member is vital to ensuring the U.S. military achieves its mission.



Crew chiefs assigned to the 386th Expeditionary Aircraft Maintenance Squadron "Blue" Aircraft Maintenance Unit perform a C-130 Hercules propeller swap Ali Al Salem Air Base, Kuwait, June 25, 2020. (U.S. Air Force photo)



Challenge 9. Improving Financial Management and Budgeting

INTRODUCTION AND OVERVIEW

The DoD's $705 billion budget represents a significant portion of the $1,486 trillion in discretionary spending found in the Federal budget, yet longstanding financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information needed for accurate budget forecasting. Additionally, the projected lack of budget growth, coupled with competing DoD priorities, makes it especially important that the DoD make programmatic and budgeting decisions based on a holistic and data-informed enterprise view of missions, requirements, risks, and the potential impacts of reduced resources. However, the DoD's current inability to produce reliable, timely, and useful financial and managerial information impedes the DoD's operating, budgeting, and decision making.

On the FY 2019 Agency-Wide Basic Financial Statements, the DoD OIG issued a disclaimer of opinion, indicating it was unable to obtain sufficient evidence on which to base an opinion. The DoD OIG also audited or oversaw the audits of the 23 DoD Components, while seven additional audits were completed by independent public accounting firms who were contracted with and monitored by the audited entity's Office of Inspector General or internal audit function. These 30 audits resulted in:

- 11 unmodified opinions, which are sometimes referred to as clean opinions and are issued when the auditor concludes that management has presented the financial statements fairly and in accordance with Generally Accepted Accounting Principles.
- 1 qualified opinion, which is issued when the auditor concludes that there are misstatements in the financial statements that are material to the financial statements but are not significant to the overall presentation of the financial statements.
- 18 disclaimers of opinion, which are issued when the auditor is unable to obtain sufficient evidence on which to base an opinion.
- 25 DoD agency-wide material weaknesses, such as Financial Management Systems and Information Technology; Inventory; Property, Plant, and Equipment; Real Property; Fund Balance With Treasury; and Financial Statement Compilation.

- 3,472 notices of findings and recommendations (NFR) to the DoD and its Components describing weaknesses in the DoD's accounting and business processes, financial reporting, and information technology (IT) systems. NFRs communicate to management the identified weaknesses, the impact of these weaknesses on the financial management processes, the reasons the weaknesses exist, and the recommendations for correcting the weaknesses. As of September 30, 2020, the FY 2020 financial statement auditors had closed 467 FY 2019 NFRs, reissued 1,695 FY 2019 NFRs, and issued 294 new NFRs.

It is critical that the DoD fix the weaknesses and deficiencies identified in the audits in order to operate more efficiently and show that it is being a good steward of taxpayers' money. The DoD will also operate more effectively as DoD senior leaders have access to reliable financial information to inform their resourcing decisions. Management Challenge 6, "Transforming Data Into a Strategic Asset," further discusses how data and information are integral to preserving and expanding the U.S military's competitive advantage and defending the United States.

IMPORTANCE OF FINANCIAL AUDITABILITY

Audits of the financial statements of the DoD and its Components provide transparency on the DoD's use of its resources, test financial information for accuracy, evaluate IT and cyber systems for compliance with specified requirements, and help improve DoD operations and decision making. The audits also provide Congress and the public with an accurate assessment of how the DoD spends its funds. In addition, the audit reports lay out the specific weaknesses identified during the audit that need to be addressed by the DoD.

Reviewing IT systems and cybersecurity is a significant function of financial statement audits. Many of the systems critical to financial management and reporting are also used for operational purposes. Therefore, testing DoD IT systems and interfaces between IT systems during the financial statement audits can identify vulnerabilities in those systems and result in recommendations to improve the DoD's cybersecurity. Without effective internal controls and proper cybersecurity, the systems that the DoD relies on to support military operations could be compromised, potentially undermining DoD operations.

Financial statement audits can also help DoD management improve its operations. The audits provide feedback regarding the effectiveness of each reporting entity's business systems, processes, and controls. Improved business systems, processes, and controls can assist the DoD in more accurately forecasting and determining the most efficient and effective uses of its funds. At the 2020 Defense News Conference, the Deputy Secretary of Defense stated, "[T]he audit drives the Department toward more accurate data." For instance, because the U.S. Transportation Command was unable to adequately document business processes during the FY 2018 audit, the auditors determined it was inefficient to perform more than limited tests. However, during the FY 2019 audit, the U.S. Transportation Command provided the auditors with adequate supporting documentation for its non-payroll and revenue transactions, which enabled the auditors to perform 113 non-payroll and 63 revenue business process reviews.[122]

[122] DoD OIG, "Understanding the Results of the Audit of the DoD FY 2019 Financial Statements," January 28, 2020.

In short, the financial statement audits can enable improvements to operations through more efficient business systems, processes, and controls, and they can result in more accurate and complete information from the DoD Components. With more accurate and complete information in the financial statements, the DoD can improve its strategic decisions, such as allocating resources, deploying new systems, and implementing new policies.

FINANCIAL MANAGEMENT CHALLENGES IDENTIFIED DURING FINANCIAL STATEMENT AUDITS

Although the DoD and several DoD Components made progress in improving their financial management during the FY 2019 audit and the ongoing FY 2020 audit, more work is required to address the financial management challenges facing the DoD.

To improve operational efficiency and budget forecasting and achieve a clean audit opinion, DoD managers must establish more effective financial management processes, beginning with addressing the material weaknesses identified by the auditors. More effective financial management processes would not only help ensure that DoD financial statements are free from material misstatement, but would also lay the foundation for benefits that would be realized over time. For example, since FY 2013, the DoD has resolved 74 percent of DoD OIG audit recommendations related to improper payments, which has improved its business processes, steadily improved its overall compliance with laws, and moved closer to meeting the President's Management Agenda, Cross-Agency Priority Goal 9, "Getting Payments Right."

DOD AUDIT PRIORITIES

The DoD is developing and completing corrective actions using material weaknesses to prioritize remediation activities and move the DoD closer to a clean audit opinion. To sustain and build on progress made in FY 2019, the Secretary of Defense called on the DoD to remain focused on audit priorities, including the following:

- Information Technology,
- Real Property,
- Inventory and Related Property,
- Government Property in the Possession of Contractors,
- Fund Balance With Treasury, and
- Financial Reporting Internal Controls.

Information Technology. Ineffective IT system controls can result in significant risk to DoD operations and assets. For example, payments and collections could be lost, stolen, or duplicated as a result of weak IT controls. In addition, critical operations, such as those supporting national defense and emergency services, could be disrupted through weak IT controls. Across multiple DoD Components, the auditors found significant control deficiencies regarding IT systems, specifically:

- security controls were not regularly monitored or tested for effectiveness,
- access rights and responsibilities were not appropriately restricted according to segregation of duties policy,
- configuration changes to IT systems were not monitored to ensure the changes were appropriate, and
- reconciliations were not being performed between systems to verify the completeness and accuracy of data transferred between systems.

The DoD is pursuing several initiatives to address weaknesses related to IT systems. For example, in FY 2019 personnel from the Office of the Under Secretary of Defense (Comptroller)/ Chief Financial Officer, the Office of the Chief Management Officer, and the Office of the Chief

Information Officer partnered to identify the root causes of IT system weaknesses and begin remediating these weaknesses. In July 2019, these offices issued a joint memorandum instructing DoD Components to take action on audit deficiencies with both a high audit impact and high cybersecurity impact. The DoD continues to have difficulties with confirming that controls exist to ensure that DoD data is shared completely and accurately between systems, and auditors continue to find control weaknesses related to the processes of sharing information between financial-related systems.

Real Property. In FYs 2019 and 2020 the DoD was unable to provide an agency-wide universe of its real property, meaning DoD leadership did not have the ability to identify all of its buildings and structures. Real property includes such things as land, administrative buildings, runways, warehouses, water supply systems, aircraft hangars, and medical treatment facilities. The DoD made some progress in this priority area in FY 2019. For example, the Navy revised policies for providing evidence for all above-ground real property on its bases, which the auditors validated during the audit. In addition, the Navy achieved a 99-percent pass rate for a judgmental sample related to completeness that was performed by the auditors, meaning the auditors concluded that the list of real property tested was complete.

The DoD plans to complete a full existence and completeness baseline to ensure 100-percent reconciliation of its buildings and structures to the accountable property systems of record by December 31, 2020. In addition, the DoD plans to complete the transfer of financial accounting responsibilities for all real property to the Military Services and Washington Headquarters Services by June 30, 2021. The DoD reported $172.6 billion of buildings, structures, and facilities in the FY 2019 DoD financial statements, which represents a significant amount of assets and DoD resources.[123] Although the DoD and its Components are taking meaningful actions, continued effort is required to ensure that all property is accounted for.

Inventory and Related Property. Inadequate controls over inventory can have a direct impact on DoD operations. Inventory and related property consists of spare parts, clothing, and textiles; operating materials and supplies, such as ammunition, tactical missiles, and aircraft configuration pods; and stockpile material, such as aluminum and tin. In FY 2019, auditors found that numerous DoD Components lacked policies, procedures, controls, oversight, and documentation related to providing assurance over the existence, completeness, and valuation of inventory. For example, auditors found that items selected for testing:

- had been moved or used but were still in the inventory records;
- were found in the warehouse, but not listed in the inventory records;
- were recorded as being in good condition but were actually unserviceable; and
- did not have supporting documentation to demonstrate ownership.

Inaccurate information in financial reporting of inventory can have significant consequences. For example, if a Military Service believes it has a low quantity of a spare part for an aircraft based on a service provider's inaccurate report, or does not review the inventory held by others, the Service may decide to order additional parts that it does not need, which is a waste of funds. Conversely, if the Service inaccurately believes that it has a sufficient quantity of spare parts for

[123] The value of buildings, structure, and facilities is based on net book value disclosed on FY 2019 DoD Agency-Wide Financial Statements.

an aircraft when it actually does not, this may result in shortfalls of the parts and the inability of aircraft to be repaired rapidly, which can affect readiness. Accurate accounting of inventory is critical to ensuring operational readiness.

Streamlined business processes that incorporate sound financial management practices, such as visibility of assets, will result in cost avoidance and improved operational efficiencies. For example, personnel at the Navy's Fleet Logistics Center Jacksonville in Florida conducted a 10-week exploratory assessment of materiel and identified $81 million in materiel not tracked in the system that was available for immediate use, decreasing maintenance time and filling 174 requisitions, including 30 that were high-priority. They also eliminated unnecessary equipment, freeing up approximately 200,000 square feet (about 4.6 acres) of warehouse space. In another example, auditors determined a 100-percent pass rate for the universe of Operating Materials and Supplies for completeness at 60 sites across the DoD. In FY 2019, Air Force Audit Agency personnel tested 1,511 military equipment assets, with a net book value of $19.3 billion located at 27 sites, for completeness and found no exceptions. The Army also made progress in asset accountability in FY 2019. At Tooele Army Depot in Utah, auditors tested a universe of 3.5 million items and found no exceptions. These examples show how the DoD is making progress toward full auditability.

The DoD and its Components are performing physical counts of all Working Capital Fund inventory and all General Fund munitions, ordnance, and uninstalled engines in their possession until a baseline is established and internal controls are in place and operating effectively. According to the June 2020 DoD Financial Improvement and Audit Remediation Report, in FY 2020, the Navy plans to conduct a 100-percent physical inventory of all materiel to improve accountability and support readiness objectives. As of September 30, 2020, the Navy had identified and added nearly $2.4 billion worth of inventory, operating materials and supplies, and general equipment to the Navy supply chain and made the inventory available across the Navy. These items were subsequently used to fill over 12,000 requisitions, totaling $49.8 million in materiel, and resulted in the disposal of $34.2 million unneeded items. While the DoD and its Components have improved asset accountability, the DoD continues to experience challenges in providing the auditors assurance over the existence, completeness, and valuation of inventory recorded in financial statements.

Government Property in the Possession of Contractors. This was identified as a material weakness during the FY 2018 audit and continued to be a material weakness for the DoD in FY 2019. Contractors may hold Government property that is directly acquired by the contractor or furnished by the Government to complete production or services on behalf of the DoD. The DoD lacks the policies, controls, oversight, and documentation required to accurately report its property in the possession of contractors.

Without accurate records, the DoD could direct one contractor to acquire property while directing another contractor to dispose of or donate the same type of property, wasting money and resources. In FY 2020, the DoD planned to review its policies, procedures, controls, and supporting documentation related to Government property in the possession of contractors to ensure proper oversight and visibility. In addition, the DoD began incorporating standard property management policies, procedures, and metrics into contract terms and conditions to enable proper accounting and accountability over Government-furnished property and develop go-forward methodology to capture all Government-furnished property. Finally, the DoD and its Components have begun a concerted effort to physically count, record,

and baseline their property in the possession of contractors. The DoD expects these initiatives to be complete by FY 2021. These corrective actions will greatly improve the accuracy and timeliness of DoD records.

Fund Balance With Treasury. DoD leadership continues to make spending decisions without knowing the accurate balance of funds available with the Treasury. The Fund Balance With Treasury is an account maintained by the Department of the Treasury that reflects the cash available for the DoD to spend. Deposits and payments by DoD Components increase or decrease the balance in the account. The auditors noted several deficiencies in the design and operation of internal controls for Fund Balance With Treasury, resulting in a DoD-wide material weakness in both FYs 2018 and 2019. The DoD has implemented extensive corrective actions, including reducing unsupported adjustments to the balances; completing reconciliations and resolving several reconciliation differences between the DoD Components and Department of the Treasury; and resolving many of the variances greater than 60 days in temporary-holding accounts, Defense-wide accounts, and other reports.

Without a proper accounting of its available funds, the DoD's spending decisions could result in over- or under-utilization of its appropriation. For example, if a DoD Component believes that it will overspend its appropriation, it might not hire sufficient staff, make needed repairs, or maintain critical equipment. Conversely, if a DoD Component believes that it will under-spend its appropriation, it could spend more funds than available, which could result in an Antideficiency Act violation.

Financial Reporting Internal Controls. The DoD and its Components lacked adequate oversight and monitoring of financial reporting internal controls to identify and resolve deficiencies that could impact their financial statement balances and related disclosures in FYs 2018 and 2019. Their planned corrective actions include improving financial reporting internal controls with sufficient oversight and monitoring to ensure effectiveness; implementing and documenting financial reporting internal controls; and working with service providers to document and implement complementary user entity controls. Although the DoD made progress toward the remediation of the oversight and monitoring material weakness, continued oversight and monitoring by the DoD and DoD Component senior leadership is critical to progress on developing sustainable solutions.

TIMELY AND ACCURATE ACCOUNTING INFORMATION FOR DECISION MAKERS

The projected lack of budget growth, coupled with competing DoD priorities, requires the DoD to make choices based on a data-informed holistic enterprise view of missions, requirements, risks, and the impacts of reduced resources. DoD leadership needs accurate accounting information to make timely resourcing decisions to ensure the DoD can effectively execute its mission, buy and sustain its weapon systems, and invest in its workforce. These resourcing decisions are further complicated due to the cost of responding to unplanned events such as the coronavirus disease–2019 (COVID-19) pandemic.

The DoD budget is projected to remain relatively flat compared to prior years, which means that the DoD will have to prioritize programs to make the best use of the available funding. For FY 2020, the DoD received a total of $695.1 billion, excluding the $10.5 billion emergency funding to combat the COVID-19 outbreak. In his proposed budget, the President requested a total of $718 billion for the DoD in FY 2021. Based on estimates provided in the 2020 Future Year Defense Plan,

total funding would be relatively level through FY 2024, averaging about $700 billion per year in 2020 dollars.[124]

To further identify savings and efficiencies within the DoD, Secretary Esper implemented a Defense-Wide Review in fourth quarter FY 2019. The process involved personnel from the Military Services and Defense Agencies performing a line-by-line examination and validation of their budgets.[125] Senior DoD officials stated that the Defense-Wide Review identified $5.7 billion in savings, which will be used to fund National Defense Strategy priorities, including research into hypersonic weapons, artificial intelligence and big data, fifth-generation communications technologies, nuclear enterprise modernization, space, missile defense, and response force readiness.

Timely and accurate data is necessary not only to pass the annual financial statement audit, but more importantly, to inform senior leader resourcing decisions, such as those made during the Defense-Wide Review. Similarly, the financial statement audits are an independent insight into what is working in the DoD and may identify opportunities for the DoD to improve. The audits' return on investment will continue to increase as remedies are implemented in the DoD and access to quality accounting information improves.

Loss of Institutional Knowledge. The DoD faces significant challenges as it works to replace the growing cadre of retirement-eligible senior civil servants in its financial management workforce with new personnel to sustain the DoD's efforts to earn a clean opinion on its financial statement audit.

As experienced personnel retire, the civilian workforce is losing its institutional knowledge, which affects its ability to improve the financial management and controls needed for reliable DoD budget forecasts. In March 2019, the Government Accountability Office High Risk List specifically mentioned in the DoD Financial Management area that DoD financial management staff remain insufficient in number, qualifications, and expertise.[126] The DoD has significant challenges ahead with maintaining continuity of leadership, personnel recruiting, training, and retaining a skilled workforce, including financial management personnel.

CONCLUSION

Reliable budget forecasts and operational efficiency require sound financial management and reporting. Sound financial management and reporting require DoD managers to design and implement effective internal controls. The DoD should prioritize implementing the recommendations contained in auditor-issued NFRs based on the seriousness of the internal control deficiency. Prioritizing in this manner will reduce the time the DoD needs to achieve unmodified, or clean, audit opinions on the Component and Agency-Wide and financial statements. Most importantly, these improvements will result in more optimized operations, corresponding cost savings that can be reallocated to higher priorities, and increased confidence from Congress and the public.

[124] Congressional Budget Office, "Long-Term Implications of the 2020 Future Years Defense Program," August 9, 2019.

[125] DoD, "Financial Improvement and Audit Remediation Plan Status Report," June 2020.

[126] Report No. GAO 19-157SP, "High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas," March 2019.

A drill instructor with Oscar Company, 4th Recruit Training Battalion, adjusts the Marine's cover as the platoon conducts its final uniform inspection on Marine Corps Recruit Depot Parris Island, South Carolina. May 1, 2020. (U.S. Marine Corps photo)

Challenge 10. Promoting Ethical Conduct and Decision Making

INTRODUCTION AND OVERVIEW

In an August 2019 memorandum, the Secretary of Defense acknowledged that the DoD enjoys the highest trust and confidence of the American people "because we live by core values grounded in duty and honor that influence how we think and act. The decisions we make every day must reaffirm our commitment to ethical conduct—doing what is right, without hesitation."[127] He explained that ethical conduct and decision making build principled, self-disciplined teams, strengthen and build new alliances, and are fundamental to sustaining a professional organization. The Secretary wrote in his memorandum that "[t]he Department's mission imparts a special responsibility on each of us to serve with the utmost integrity" and directed DoD leaders to "[c]reate an open, transparent environment that reinforces values-based decision making and action. And always treat everyone with dignity and respect." Actions by DoD personnel that are counter to these principles can erode the special trust and confidence in the DoD, undermine good order and discipline, and make it more difficult for the DoD to secure the congressional and public support necessary to address the global threats facing the United States.

DoD personnel must strive to act above reproach, make decisions consistent with organizational values, and ensure the welfare of those around them. With the continued development of advanced technologies, such as artificial intelligence (AI), the DoD must remain aware of potential ethical pitfalls when employing these technologies. Similarly, the DoD needs to continue aggressively pursuing ways to eliminate sexual assault and sexual harassment in the force, and hold accountable those who violate the DoD's values, ethical principles, and standards.

[127] Secretary of Defense Memorandum, "Reaffirming Our Commitment to Ethical Conduct," August 19, 2019.

ETHICAL PRINCIPLES FOR THE USE OF AI

AI is a rapidly growing technological field with potentially significant implications for national security. AI is defined as the capability of computer systems to perform tasks that normally require human intelligence. Over the last 20 years, the field has grown exponentially, from smart phones using facial recognition to voice interaction with computers and tailored marketing on social media. In November 2019, the Secretary of Defense stated, "Advances in AI have the potential to change the character of warfare for generations to come. Whichever nation harnesses AI first will have a decisive advantage on the battlefield for many, many years. We have to get there first."

While AI has potential to revolutionize how war is conducted by rapidly speeding up the collection and processing of data and information to facilitate analysis and decision making, DoD leaders must balance the need to leverage this new capability with identifying and evaluating any ethical risks or unintended consequences resulting from its use. AI and machine learning have great potential, but if the speed of development is prioritized over ethical safeguards, the resulting AI technology could be less safe, and resultant decisions or actions less trustworthy. For example, regarding the decision to fire a weapon, preserving human involvement in the decision is critical to ensuring responsibility for the use of AI and in retaining the ability to disengage or deactivate deployed weapon systems to prevent unintended consequences. Compromised

Detachment 24 student pilots train on a virtual reality flight simulator as part of the Pilot Training Next program March 5, 2020, at Joint Base San Antonio-Randolph, Texas. (U.S. Air Force photo)

AI-enabled decision-making capabilities could make decisions too quickly or the systems might not be able to adapt to the inevitable complexities of war. As a result, AI might not be able to accurately distinguish between combatants and noncombatants, or threats and system anomalies. These problems could be magnified if systems are fielded before being adequately tested, or if adversaries succeed in spoofing or hacking into them. The collection of large amounts of data also calls into question which data is appropriate for the DoD to collect, use, store, and secure. Without the appropriate ethical and security safeguards, the combination of massive amounts of data and the use of AI could result in a significant invasion of privacy and could give the U.S. Government unprecedented information, control, and power over American citizens.

The DoD must also understand and be prepared to address the concerns the public has with how the DoD could use AI. For example, in March 2019, Google allowed its image recognition program portion of a DoD contract to expire as a result of a petition from employees. Over 3,000 Google employees signed a petition urging Google to avoid warfare technology that puts Google's reputation at risk and is counter to its values. To maintain public trust and industry participation, the DoD must continue to show the Defense Industrial Base and the public at large that it acknowledges and considers the concerns.

Many experts fear that the pace of AI technology is moving faster than the speed of policy development. Former Chairman of the House Armed Services Committee, Representative Mac Thornberry, echoed this sentiment, stating, "It seems to me that we're always a lot better at developing technologies than we are the policies on how to use them." In 2018, the Defense Innovation Board made recommendations to the DoD regarding the use of AI and other technologies, stating, "rigorous work is needed to ensure new tools are used responsibly and ethically."[128] Prompted by these recommendations, on February 24, 2020, the DoD officially adopted a series of ethical principles for the use of AI in the advancement of trustworthy AI technologies. These principles build on the U.S. military's existing ethics framework and focus on five key areas: responsibility, equitability, traceability, reliability, and governability. In general, the DoD recognizes the importance of exercising appropriate judgment in the development and use of AI capabilities, and acknowledges potential unintended biases and consequences that arise when leveraging new opportunities.

The DoD's challenges regarding the development of AI are discussed further in Management Challenge 2, "Building and Sustaining the DoD's Technological Dominance," and Management Challenge 8, "Strengthening and Securing the DoD Supply Chain and Defense Industrial Base," discusses how AI is being used in logistics to improve readiness in the DoD.

SEXUAL ASSAULT IN THE MILITARY

Sexual assault continues to be an enduring ethical challenge despite significant focus by DoD senior leaders and the establishment of the DoD Sexual Assault Prevention and Response Office (SAPRO) in 2005. SAPRO is responsible for developing and implementing prevention and response programs. In 2014, retaliation for reporting sexual assault became a focus of SAPRO's programmatic efforts after a 2014 RAND report stated that 62 percent of active duty women who reported sexual assault perceived some sort of retaliation.

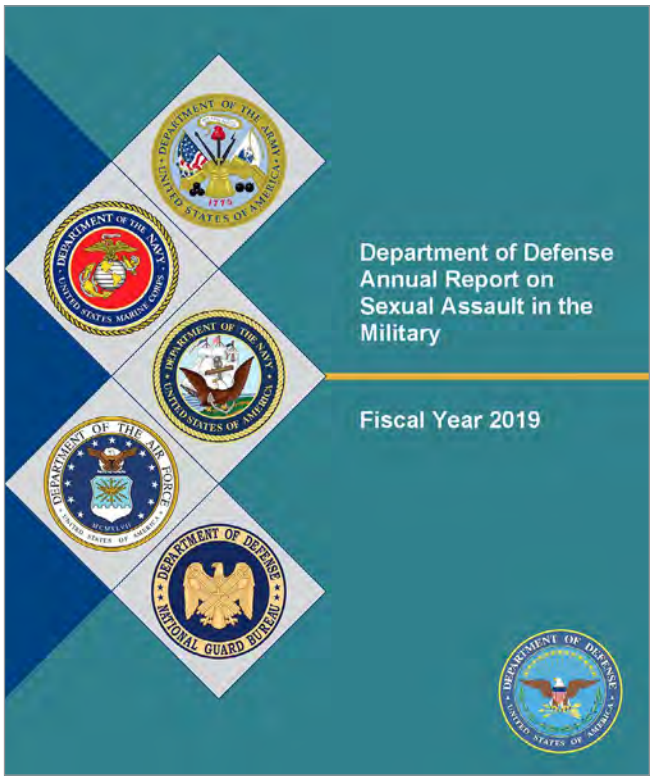
[128] DoD, "Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2019," April 17, 2020.

In 2016, the DoD OIG took sole responsibility for investigating complaints of retaliation for reporting sexual assault under the Military Whistleblower Protection Act.

In April 2019, SAPRO released the DoD's Prevention Plan of Action for 2019-2023, which established a comprehensive prevention process and prevention system, as well as specific actions the DoD, Military Services, and National Guard Bureau will take to realize effective prevention in every military community.

On April 20, 2020, the DoD released its FY 2019 Annual Report on Sexual Assault in the Military, presenting statistics and analysis of reports of sexual assault during FY 2019. The report indicated that while there are a number of positive trends in the DoD, including survey groups that feel the DoD's plan of action is targeting the right personnel and activities to drive change, the number of reported sexual assaults still grew by 3 percent.[129] In addition, the annual report stated that some active duty members continued to fear retaliation for reporting an experience of sexual assault, which may indicate more work is necessary.

The National Guard has also recently been singled out by Members of Congress and the press for its failure to appropriately handle incidents of sexual assault. Over the last year and a half, Guard leadership from at least three states has either resigned or been removed amidst allegations, investigations, or findings concerning its mishandling of investigations of sexual assault and misconduct, and allegations of widespread whistleblower retaliation for reporting sexual assault and harassment. In 2019, in an effort to address what may be systemic issues within the Guard, the Chief of the National Guard Bureau published a letter to the adjutants general of each state and territory's Guard that emphasized, "As senior military leaders, we share the responsibility to establish safeguards to protect our most valuable assets: our National Guard Members, their families, and civilian employees."



The number of investigations of allegations of retaliation for reporting a sexual assault being conducted by the DoD OIG decreased slightly in FY 2020 from FY 2019. However, retaliation for reporting a sexual assault remains a moral, ethical, and legal issue for the DoD. Not only does retaliation discourage victims from reporting allegations, it also discourages others from providing important information about an alleged incident. In the past year, the DoD OIG has received 76 complaints of reprisal related to reporting a sexual assault, initiated 9 new investigations, and closed 10 investigations. In one case, an Air Force lieutenant colonel and

[129] DoD, "Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2019," April 17, 2020.

senior master sergeant did not recommend an Air Force staff sergeant for reenlistment and denied transition leave to the staff sergeant in reprisal for the staff sergeant having reported unrestricted reports of sexual assaults to the chain of command on multiple occasions. Events like this are indicative that the DoD still has challenges related to sexual assault prevention and ensuring that those who report a sexual assault are protected from reprisals and becoming the target of ostracism or maltreatment.

Congress continues to express concerns with sexual assault in the military. The National Defense Authorization Act (NDAA) for FY 2020, for example, contained nearly 20 new requirements, including the development and issuance of a comprehensive policy to reinvigorate the prevention of sexual assault involving service members. It requires, among other things, programs for encouraging and promoting healthy relationships among service members, empowering and enhancing the role of non-commissioned officers in the prevention of sexual assault, fostering social courage to encourage and promote intervention in situations, and addressing behaviors that are included in the continuum of harm that frequently result in sexual assault. The DoD needs to continue focusing on protecting others, fostering an environment of dignity and respect, and holding accountable those who commit sexual assault and retaliate against those who report it.

SEXUAL HARASSMENT IN THE DOD

DoD Instruction 1020.03 states that sexual harassment is conduct that "involves unwelcome sexual advances, requests for sexual favors, and deliberate or offensive comments or gestures of a sexual nature."[130] It may also include inappropriate actions such as sexist jokes, gender discrimination, hazing, cyber bullying, and other behaviors that contribute to a culture that is seen as tolerant of sexual assault. While sexual harassment is not unique to the DoD, as evidenced by the #MeToo movement, the DoD must keep pace with changing societal norms or risk erosion of the public's trust and confidence in DoD leadership and undermining good order and discipline in an organization.

Despite the heightened emphasis on countering sexual harassment and other sexual misconduct, the effects of these acts on morale and readiness remain a persistent challenge for the DoD. In the FY 2013 NDAA, Congress required that within 120 days of taking command and at least annually thereafter, a climate assessment of the command or unit be conducted, to allow service members "to express their opinions regarding the manner and extent to which their leaders, including commanders, respond to allegations of sexual assault and complaints of sexual harassment and the effectiveness of such response." The following year, Congress required the Secretary of Defense to ensure the results of command climate assessments are provided to the relevant individual commander and to the next higher level in the chain of command, to increase accountability. Although the Military Services have implemented policies requiring climate assessments, it is unclear whether those assessments have led to actions that hold commanders accountable for poor command climates.

According to the Workplace and Gender Relations Survey of Active Duty Members, published in 2018, poor workplace climate

[130] DoD Instruction 1020.03, "Harassment Prevention and Response in the Armed Forces," February 8, 2018.

remained a top risk factor for sexual harassment. The results indicated that commands with a prevalence of sexual harassment behaviors were more likely to have a higher rate of reported sexual assaults. With nearly a quarter of active duty women reporting in the survey that in the past year they had experienced repetitive, offensive, unwanted sexual attention, comments, and jokes, the DoD potentially faces a retention challenge.[131]

During an August 2020 visit to Fort Hood, Texas, the Secretary of the Army stated, "The numbers [of crime] are high here. They are the highest, in most cases, for sexual assault and harassment and murders for... the U.S. Army." The Secretary made this comment as service member disappearances, deaths, and experiences of sexual harassment and sexual assault at Fort Hood over the last year have drawn significant social and political attention. Since June 2020, Members of Congress and DoD leaders have requested various reviews of the Army's Sexual Harassment/Assault Response and Prevention (SHARP) Program at Fort Hood; the command climate at the base, including Fort Hood's chain of command; and the treatment of women and individuals of color in the military. These requests arose in response to the brutal murder in April 2020 of an Army specialist at Fort Hood, whose family claims that she had told them she was being sexually harassed by a fellow soldier, but never informed her chain of command about the harassment for fear of reprisal. The Army replaced the general officer serving as the acting commander of Fort Hood and suspended his next planned command assignment pending the results of an investigation.

The DoD maintains a culture-focused approach to addressing sexual harassment. The DoD's Prevention Plan of Action for 2019-2023 report cites the results of several working groups that developed a list of knowledge, skills, and attitudes required in new leaders to effectively address negative command climate issues that may contribute to sexual harassment.[132] The next step in the Plan is for the DoD to incorporate these principles into education and training efforts at all levels.

Based on the substantiation of allegations in closed administrative investigations, the DoD continues to deal with the negative effects of sexual harassment on an individual and organizational level. The DoD OIG recently substantiated allegations against a member of the Senior Executive Service, who over a 7-year period repeatedly sought out and made deliberate, unwelcomed physical contact with subordinate employees. In another substantiated case, a brigadier general disparaged, bullied, and humiliated subordinates, devalued women, and created a negative work environment. These two examples, while not indicative of the entire DoD, do serve to highlight that the DoD must continue its efforts to eradicate this type of behavior.

Sexual harassment and other misconduct remain a persistent problem in the military. If the DoD fails to address these behaviors and reinforce a culture of respect for all service members and DoD employees, it will put individuals' lives in danger, undermine good order and discipline, and risk losing the public's trust and confidence in the DoD.

[131] DoD Office of People Analytics Report No. 2019-027, "2018 Workplace and Gender Relations Survey of Active Duty Members Overview Report," May 2019.

[132] DoD, "Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2019," April 17, 2020.

UPHOLDING CORE VALUES

In addition to responding to individual cases of ethical misconduct, the DoD has been examining the culture in the U.S. special operations forces since 2011. These highly skilled operators have attracted widespread scrutiny in recent years for their individual conduct and leadership's apparent unwillingness to hold individuals accountable. In August 2019, the Commander of U.S. Special Operations Command (USSOCOM) directed a Comprehensive Review to assess "culture and ethics, to gather insights and observations from across the force, at all levels."[133] According to the final report published in January 2020, USSOCOM culture "prioritizes force employment over leadership, discipline and accountability." This mindset harms leadership development, discipline and accountability, and it enables misconduct and unethical behavior. The report acknowledged, "[T]he force exhibits—at times—high risk behavior which has contributed to some of the recent incidents of misconduct and unethical behavior."

The FY 2017 NDAA required the Secretary of Defense to expand the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict's roles and responsibilities in the oversight of special operations forces.[134] In response to the report, the USSOCOM Commander told reporters, "We need to improve our leader development programs and improve accountability in our training and management processes … Leaders drive culture, and maintaining a healthy and high performing culture requires present and actively involved leadership." USSOCOM's 2020 Comprehensive Review stated that a review team had "uncovered not only potential cracks in the [special operations forces] foundations at the individual and team level, but also through the chain of command, specifically in the core tenets of leadership, discipline and accountability."[135] Upholding values and holding others accountable for violations is critical for the DoD to ensure it is promoting and demonstrating ethical conduct and decision making.

CONCLUSION

Ethical conduct and decision making are essential to upholding the values of the DoD and its Components. Despite the tremendous potential for AI and other advanced technologies, the DoD must consider any ethical issues related to implementing emerging technologies. Service members and DoD civilians must take care of each other and demonstrate behaviors that uphold the dignity and respect of others. Equally important is accountability. Leaders must hold people accountable when they violate rules, regulations, and laws, especially as it relates to sexual harassment, sexual assault, or other ethical breaches. The DoD must work to eliminate these behaviors and remain vigilant to preserve the trust and confidence of the American people.

[133] DoD, "United States Special Operations Command Comprehensive Review," January 23, 2020.

[134] Report No. GAO-19-386, "Special Operations Forces: Additional Actions Are Needed to Effectively Expand Management Oversight," May 13, 2019.

[135] DoD, "United States Special Operations Command Comprehensive Review," January 23, 2020.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Coordinator's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. For more information, please visit the Whistleblower Protection Coordinator's webpage at:

https://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Protection-Coordinator/.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098