# Accessible Version

Security

# **CHALLENGES FACING DOD IN STRATEGIC** snapshot **COMPETITION WITH CHINA**

Surface and Undersea

China has robust offensive and

defensive capabilities aimed at

the first island chain, including

carriers 1,500 km from China's

gaining maritime superiority within

ballistic missiles able to target aircraft

coast. China also has the largest navy

**Operations** 

# **FEBRUARY 2022**

According to the 2021 Interim National Security Strategic Guidance, China is increasingly assertive and the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system.

From a defense perspective, China is a significant and long-term security threat and the pacing threat in most areas, according to the Secretary of Defense. However, the Department of Defense (DOD) has also highlighted weaknesses and challenges facing China. For example, the Defense Intelligence Agency reported that China, as a large developing country, still faces multiple complex security challenges including several regional territorial disputes.

# CHALLENGES TO U.S. NATIONAL SECURITY

China has greatly strengthened its military capabilities over the last 20 years and its stated goal is to have a "world-class" military by the end of 2049, according to DOD. Today, China has transformed what was an obsolete military into one that can challenge the U.S. military across the spectrum of conventional and unconventional capabilities. Below are examples of concerns highlighted by DOD and GAO.

## Figure 1: Selected Chinese Military Capabilities

#### **Anti-Access/Area-Denial**

China is expanding its capability to counter third-party (i.e., U.S.) intervention during a large-scale, theater campaign such as a Taiwan contingency. This anti-access/area-denial capability includes long-range precision strike capabilities (ballistic and cruise missiles) able to reach U.S. logistics and power projection assets in the region, including Guam, and robust air defenses that reach over 550 km from its coast.



Source: GAO analysis of Department of Defense information; Map Resources (map). | GAO-22-105448



# **GAO REVIEW OF KEY DOD ACTIONS**

GAO has a large body of work that documents the steps DOD has taken as it refocuses on strategic competition and recommends ways the department can bolster national security. GAO has long reported on China's military modernization to assist the Congress in decisions it faces regarding China. GAO has more recently reported that China may challenge U.S. access to air, space, cyberspace, and maritime domains.

GAO has reviewed various DOD approaches and capabilities for countering these challenges. For example, the Navy is in the early stages of determining how it will provide <u>battle damage repair</u> during a great power conflict. Additionally, DOD has developed lists of cyber techniques that adversaries use most frequently and pose significant risk to the department, and identified practices to protect DOD networks and systems against these techniques. GAO has also reviewed DOD efforts to reform its acquisitions to develop and field new capabilities more quickly and DOD-sponsored studies on <u>contested mobility</u>—the ability to transport equipment and personnel in a contested operational environment. GAO has also reported on DOD's efforts to develop advanced weapons systems such as hypersonics.

### **RELEVANT GAO WORK**

GAO has published numerous unclassified and classified reports that can help inform decision makers in Congress and DOD as they weigh options for how to best respond to the national security challenges posed by China. Figure 2 identifies a number of these unclassified reports and how they relate to five specific challenge areas DOD faces.

#### Figure 2: Related Unclassified GAO Work



Emerging Threats: Federal agencies have identified long-range, emerging issues which threaten U.S. national security. These include changes in the political and military interests of potential adversaries such as China, as well as developments in dual-use or weapons technologies. GAO-19-204SP

Military Readiness: Potential adversaries, including China, now contest all domains. From fiscal years 2017 through 2019, U.S. military readiness increased in the ground domain and declined in the sea domain, while readiness ratings in the space, air, and cyber domains were mixed. <u>GAO-21-279</u> Weapon Systems Review: DOD is investing more than \$1.8 trillion on new systems, but many face cost, schedule, and other issues. <u>GAO-21-222</u>

Nuclear Triad: Most U.S. nuclear systems are nearing or past end-of-life dates and replacement systems are at risk of delays. DOD must manage their programs to credibly deter potential adversaries such as China. <u>GAO-21-210</u>

Contested Mobility: China will continue to improve its military and threaten DOD's mobility capability. DOD may be missing opportunities to leverage existing studies to further mitigate mobility threats. GAO-21-125

F-35: DOD needs to take steps to assess and mitigate risks associated with key supply chain-related challenges, including the F-35's central logistics system, and to determine the F-35's ability to effectively support operations in the Pacific. GAO-20-316 GAO-18-464R

Defense Planning: China will continue to pursue capabilities to counter U.S. power projection. DOD needs specific measures and milestones to gauge progress of preparations for operational access challenges or it may not operate effectively in future operating environments. GAO-14-801 Navy Readiness: Crew shortfalls contribute to sailor fatigue and safety issues, including two fatal Navy ship collisions in the Pacific Ocean in 2017. With Navy ships undercrewed by 15% on average in 2020, the Navy will be challenged to fully crew the fleet needed to counter advanced adversaries. GAO-21-366

Navy Submarines: Attack submarines provide an asymmetric advantage to gather intelligence undetected, attack enemy targets, and insert special forces, but the Navy incurred over 10,000 lost operational days from 2008 through 2018 during which these key assets provided no operational capability.

operational capability. GAO-19-229

Battle Damage Repair: The Navy is in the early stages of determining how it will provide battle damage repair during a major conflict. Without designated leadership, the Navy may be hindered in its efforts to address sustainment challenges. GAO-21-246

# Electromagnetic

Operations: DOD needs to improve oversight over electromagnetic spectrum operations to ensure superiority over potential adversaries like China and control over the battlefield. GAO-21-64

#### Weapons

Cybersecurity: DOD has struggled to ensure its weapon systems can withstand cyberattacks and should take steps to incorporate cybersecurity requirements into contracts. GAO-21-179

Cyber Hygiene: To manage the most common and pervasive cybersecurity risks from potential adversaries like China, DOD needs to take action. GAO-20-241

Defense Cybersecurity: The Defense Logistics Agency needs to address cyber-related risk management deficiencies in inventory systems critical to managing the defense supply chain. GAO-21-278

#### Satellite

Communications: China is developing capabilities that threaten DOD's satellite communications systems. DOD has analyzed alternatives to replace existing systems and concluded that it needs more information to select the next satellite communications architecture. GAO-20-80

#### Missile Warning

Satellites: The U.S. effort to replace the infrared sensor satellites used for ballistic missile warning is likely to be delayed. Program officials are aware of schedule risks, but continue to report an on-track timeline and stable cost estimates in reports to Congress. GAO-21-105249

Military Space Systems: DOD uses commercial satellites as a cheaper and faster way to host defense payloads to help defend against adversary attacks. However, DOD's knowledge on its components' use of hosted payloads is fragmented. GAO-18-493

#### DOD Critical

Technologies: DOD needs to effectively identify and ensure the consistent protection of critical technologies such as elements of artificial intelligence from adversaries. <u>GAO-21-158</u>

Defense Intelligence and Security: Additional oversight actions would position DOD to effectively guide the Defense Intelligence and Security Enterprises to better address new responsibilities in AI, among other areas. GAO-21-295

Artificial Intelligence: GAO's AI accountability framework can help DOD ensure it uses AI responsibly. GAO-21-519SP

Deepfakes: Deepfakes could be used to influence elections or incite civil unrest, or as a weapon of psychological warfare. A deepfake is a video, photo, or audio recording that seems real, but has been manipulated with Al. GAO-20-379SP

# **GAO RECOMMENDATIONS**

Congress and DOD face many choices as they determine the strategic focus of long-term competition with China, and DOD has implemented many of GAO's recommendations that could help the department better prepare. However, as of February 2022, GAO has identified additional actions that may better position DOD to address the challenges with China that DOD has not yet implemented, including recommendations shown in figure 3.

### Figure 3: Select Recommendations Identified in GAO Work as of February 2022

-	-
$\checkmark$	<ul> <li>Develop a process for measuring how issues with the F-35's central logistics systems affect its mission capable rates. <u>GAO-20-316</u></li> <li>Develop and implement a strategy for the re-design of the F-35's central logistics system. <u>GAO-20-316</u></li> </ul>
Anti-Access/ Area-Denial	<ul> <li>Evaluate the results of contested mobility studies and track the implementation of recommendations. <u>GAO-21-125</u></li> </ul>
Surface and Undersea Operations	<ul> <li>Periodically assess and update ship vulnerability models to inform battle damage repair planning efforts. <u>GAO-21-246</u></li> <li>Use collected data on sailor fatigue to identify, monitor, and evaluate factors that contribute to fatigue. <u>GAO-21-366</u></li> <li>Address the main factors contributing to maintenance delays and improve the timely completion of ship maintenance. <u>GAO-20-588</u></li> </ul>
Cyber	<ul> <li>Develop plans that comprehensively assess and identify specific Cyber Mission Force training requirements. <u>GAO-19-362</u></li> <li>Ensure that cyber hygiene initiatives are fully implemented and that completion of relevant tasks is monitored to protect the DOD network from key cyberattack techniques. <u>GAO-20-241</u></li> <li>Update Defense Logistics Agency standard operating procedures to require program offices to develop a system-specific monitoring strategy consistent with DOD's risk management framework. <u>GAO-21-278</u></li> </ul>
Space	<ul> <li>Update DOD's dated narrowband satellite communication requirements to ensure warfighters have needed communications tools in the future. <u>GAO-21-105283</u></li> <li>Develop a plan to guide implementation of DOD's recommendations for future wideband satellite systems. <u>GAO-20-80</u></li> <li>Finalize a comprehensive acquisitions strategy for space command and control systems. <u>GAO-20-146</u></li> </ul>
Artificial	<ul> <li>Identify, develop, and review metrics to assess the implementation and sufficiency of protection measures for critical technologies, including AI. <u>GAO-21-158</u></li> <li>Develop tools to enhance accountability for intelligence and security mission areas and use these tools to conduct oversight. <u>GAO-21-295</u></li> </ul>

### CONCLUSIONS

China's growing economic, diplomatic, military, and technological power—and a willingness to exercise it—pose a significant long-term challenge to the United States.

Amidst this backdrop, successful preparation for strategic competition with China will depend on continuing efforts to increase U.S. combat credibility and enhance conventional deterrence that can help prevent conflict, protect U.S. interests, and assure allies. Going forward, key policy considerations include ensuring that DOD is prepared to maintain supply chains, gather intelligence, and responsibly leverage emerging space, cyber, and AI technologies in response to potential threats.

DOD has begun to identify new ways to deploy its existing capabilities and identify new ones, and China is facing its own major challenges. The Defense Intelligence Agency reported that China is vulnerable to international and regional turmoil, terrorism, piracy, serious natural disasters, and epidemics. In addition, DOD has reported that China's military continues to have major gaps and shortcomings and has not fought a war with its current suite of capabilities. For the U.S. to be poised for success in facing threats from China, DOD will need to take timely actions and congressional oversight will be important as these efforts proceed.

Source: GAO. | GAO-22-105448

# **ABOUT GAO**

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people.

Connect with GAO on <u>Facebook</u>, <u>Flickr</u>, <u>Twitter</u>, and <u>YouTube</u>. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit <u>GAO</u> on the web.

A. Nikki Clowers, Managing Director, Congressional Relations <u>ClowersA@gao.gov</u>, (202) 512-7114

Chuck Young, Managing Director, Public Affairs YoungC1@gao.gov, (202) 512-4800

U.S. Government Accountability Office 441 G Street NW, Washington, DC 20548

This document is based on unclassified GAO audit products and may be updated as appropriate. GAO has also produced sensitive and classified products related to these topics.

For more information about this Snapshot, contact:

Cathleen A. Berrick, Managing Director, Defense Capabilities and Management BerrickC@gao.gov, (202) 512-3404

Staff acknowledgements: Brian Mazanec, Nicolaas Cornelisse, Patricia Lentini, Amie Lesser, TC Corless, Carolyn Demaree, Clarice Ransom, Jordan Tibbetts, Alexander Webb, and Bailey Wong.

Source: Earnest Tse/stock.adobe.com (cover photo).

