Highlights of **GAO-19-204SP**, a report to congressional committees

National Security

Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies

Why GAO Did This Study

The United States faces a complex array of threats to our national security, including our political, economic, military, and social systems. These threats will continue to evolve as new and resurgent adversaries develop politically and militarily, as weapons and technology advance, and as environmental and demographic changes occur. A House committee report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 included a provision for GAO to identify emerging threats of high national security consequence. This report focuses on long-range emerging threats—those that may occur in approximately 5 or more years, or those that may occur during an unknown timeframe—as identified by various respondents at the Department of Defense (DOD), Department of State (State), Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI).

To identify long-range emerging threats, GAO administered a questionnaire to 45 government organizations that assess emerging threats across DOD, State, DHS, and ODNI, and had a 78-percent response rate. GAO conducted a content analysis of the responses to identify specific threats and develop broad threat categories. To supplement the data from the questionnaire, GAO reviewed national security strategies and agency documents provided by DOD, State, DHS, and ODNI, and interviewed key agency officials. This report is a public version of a classified report that GAO issued on September 28, 2018. Information that DOD deemed classified and sensitive has been omitted.

What GAO Found

DOD, State, DHS, and ODNI independently identified various threats to the United States or its national security interests. In analyzing more than 210 individual threats identified by organizations across DOD, State, DHS, and ODNI, as well as its review of national security strategies and related documents, and interviews with key agency officials, GAO developed four broad categories for 26 long-range emerging threats that officials identified: Adversaries' Political and Military Advancements, Dual-Use Technologies, Weapons, and Events and Demographic Changes.

The figure below contains examples of the 26 threats in 4 categories—as identified by DOD, State, DHS, and ODNI—in response to GAO's questionnaire.

For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov or Brian M. Mazanec at (202) 512-5130 or mazanecb@gao.gov.

Emerging Threats As Identified by DOD, State, DHS, and ODNI

Adversaries' Political and Military Advancements

Chinese Global Expansion» China is marshalling its diplomatic, economic, and military resources to facilitate its rise as a regional and global power. This may challenge U.S. access to air, space, cyberspace, and maritime domains. China's use of cyberspace and electronic warfare could impact various U.S. systems and operations.

Russian Global Expansion» Russia is increasing its capability to challenge the United States across multiple warfare domains, including attempting to launch computer-based directed energy attacks against U.S. military assets. Russia is also increasing its military and political presence in key locations across the world.

Iranian Political and Military Developments» Iran is expanding its influence by increasing the size and capabilities of its network of military, intelligence, and surrogate forces, while increasing economic activities in other areas of the world. Iran will also likely continue to develop its military capabilities, including developing technology that could be used for intercontinental ballistic missiles (ICBM) and improving its offensive cyberspace operations.

North Korean Military Developments» North Korea is developing capabilities to strike North America and its allies with long-range missiles and may produce significant numbers of intercontinental ballistic missiles.

Foreign Government Capacity and Stability» Violent extremist organizations may proliferate in countries that have limited governing capacity and are facing conflict, which may result in a higher risk of terrorist attacks and increased demand for U.S. resources to counter them. Countries in Africa, Latin America, and the Caribbean may experience instability based on conflict, which may lead to humanitarian disasters and government collapses.

Terrorism» Violent ideologies could influence additional individuals to turn to terrorism to achieve their goals across Africa, Asia, and the Middle East. Terrorists could advance their tactics, including building nuclear, biological or chemical weapons, or increase their use of online communications to reach new recruits and disseminate propaganda.

New Alliances and Adversaries» The United States could face challenges from potential new state adversaries and non-state adversaries (e.g., private corporations obtaining resources that could grant them more influence than states).

Information Operations» Adversaries—such as Russia, Iran, and China—may engage in advanced information operations campaigns that use social media, artificial intelligence, and data analytics to undermine the United States and its allies.

Emerging Threats As Identified by DOD, State, DHS, and ODNI (Continued)

Dual-Use Technologies

Artificial Intelligence (AI)» Adversaries could gain increased access to AI through affordable designs used in the commercial industry, and could apply AI to areas such as weapons and technology.

Quantum Information Science» Quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt. Quantum computing may allow adversaries to decrypt information, which could enable them to target U.S. personnel and military operations.

Internet of Things (IoT)» The United States may face difficulties protecting networks and data as IoT grows and traditional approaches for security (e.g., encryption) may no longer effectively protect information. Adversaries could also disrupt IoT-enabled critical infrastructure and devices.

Autonomous and Unmanned Systems» Adversaries are developing autonomous capabilities that could recognize faces, understand gestures, and match voices of U.S. personnel, which could compromise U.S. operations. Unmanned ground, underwater, air, and space vehicles may be used for combat and surveillance.

Biotechnology» Actors—which may include state or non-state entities such as violent extremist organizations and transnational criminal organizations—could alter genes or create DNA to modify plants, animals, and humans. Such biotechnologies could be used to enhance the performance of military personnel. The proliferation of synthetic biology—used to create genetic code that does not exist in nature—may increase the number of actors that can create chemical and biological weapons.

Other Emerging Technologies» Actors may gain access to new technologies previously limited to militaries, such as affordable and sophisticated encryption technologies, which would hinder U.S. efforts to monitor terrorist and criminal activities. Other emerging technologies—such as additive manufacturing (i.e., 3D printing)—may be vulnerable to cyber attacks or be used to manufacture restricted materials, such as weapons.

Weapons

Weapons of Mass Destruction» An increasing number of actors may gain access to these weapons. Adversaries could steal nuclear materials from existing facilities or develop new types of biological weapons using genetic engineering and synthetic biology.

Electronic Warfare» Adversaries are developing electronic attack weapons to target U.S. systems with sensitive electronic components, such as military sensors, communication, navigation, and information systems. These weapons are intended to degrade U.S. capabilities and could restrict situational awareness or may affect military operations.

Hypersonic Weapons» China and Russia are pursuing hypersonic weapons because their speed, altitude, and maneuverability may defeat most missile defense systems, and they may be used to improve long-range conventional and nuclear strike capabilities. There are no existing countermeasures.

Counterspace Weapons» China and Russia are developing anti-satellite weapons to threaten U.S. space operations. China is developing capabilities to conduct large-scale anti-satellite strikes using novel physical, cyber, and electronic warfare means.

Missiles» Adversaries are developing missile technology to attack the United States in novel ways and challenge U.S. missile defense, including conventional and nuclear ICBMs, sea-launched land-attack missiles, and space-based missiles that could orbit the earth.

Intelligence, Surveillance, Reconnaissance (ISR) Platforms» Future advances in AI, sensors, data analytics, and space-based platforms could create an environment of "ubiquitous ISR", where people and equipment could be tracked throughout the world in near-real time. China, Russia, Iran, and North Korea are developing multiple ISR platforms.

Aircraft» China and Russia are developing new aircraft, including stealth aircraft, which could fly faster, carry advanced weapons, and achieve greater ranges. Such aircraft could force U.S. aircraft to operate at farther distances and put more U.S. targets at risk.

Undersea Weapons» Russia has made significant advancements in submarine technology and tactics to escape detection by U.S. forces. China is developing underwater acoustic systems that could coordinate swarm attacks—the use of large quantities of simple and expendable assets to overwhelm opponents—among vehicles and provide greater undersea awareness. Adversaries could achieve breakthroughs in anti-submarine warfare—such as using AI to locate U.S. submarines—or attack U.S. undersea infrastructure, which could cripple communications.

Cyber Weapons» Adversaries, such as China, Russia, Iran, and North Korea, may launch cyber attacks against critical U.S. infrastructure (e.g., electric, oil and gas, and nuclear power systems) and military infrastructure (e.g., communications and ISR platforms). Adversaries could also launch cyber attacks on the U.S. health care system, threatening patient safety by disrupting access to medical care. Finally, adversaries are also developing tools to directly attack hardware and embedded components in aviation systems, which can manipulate or destroy data.

Events and Demographic Changes

Infectious Diseases» New and evolving diseases from the natural environment—exacerbated by changes in climate, the movement of people into cities, and global trade and travel—may become a pandemic. Drug-resistant forms of diseases previously considered treatable could become widespread again.

Climate Change» Extreme weather events—such as hurricanes and megadroughts—could intensify and affect food security, energy resources, and the health care sector. Diminishing permafrost could expand habitats for pathogens that cause disease. The loss of Arctic sea ice could open previously closed sea routes, potentially increasing Russian and Chinese access to the region and challenging the freedom of navigation that the United States currently has.

Internal and International Migration» Governments in megacities (i.e., over 10 million people) across Asia, Latin America, and Africa may not have the capacity to provide adequate resources and infrastructure, and may be vulnerable to natural or man-made disasters. Mass migration events may occur and threaten regional stability, undermine governments, and strain U.S. military and civilian responses.

Source: GAO analysis of DOD, State, DHS, and ODNI questionnaire responses, agency documents, and national security strategies. | GAO-19-204SP