Report to Congressional Committees

NATIONAL SECURITY

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

December 2018

GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE
GAO-19-204SP

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

Contents

Letter 1

Background 3

DOD, State, DHS and ODNI Identified a Variety of Emerging Threats to U.S. National Security That May Occur over the Next Approximately 5 or More Years 6

- Adversaries' Political and Military Advancements 7
- Dual-Use Technologies 8
- Weapons 9
- Events and Demographic Changes 10

Agency Comments and Our Evaluation 11

List of Congressional Committees 12

Appendix I: Objective, Scope, and Methodology 13

Appendix II: DOD Comments 17

Related GAO Products 18

Abbreviations

AI	Artificial Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
ICBM	Intercontinental ballistic missile
IoT	Internet of Things
ISR	Intelligence, surveillance, and reconnaissance
NATO	North Atlantic Treaty Organization
ODNI	Office of the Director of National Intelligence
State	Department of State

December 13, 2018

Congressional Committees

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. Our adversaries may include foreign governments, violent extremists, transnational criminal organizations, and megacorporations.[1] Threats may also come from events such as pandemics, human migration, regional conflict and instability, economic inequality, or the effects of climate change and environmental issues.

A variety of national intelligence and security organizations are responsible for national security, including identifying, analyzing, and countering emerging threats. Such organizations include: the Department of Defense (DOD), the Department of State (State), the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI).

For purposes of this report, we define "threat" as an actor with capability and intent, or an event with potential capability, to harm the United States or its national security interests. We define "emerging threat" as a threat that may be newly recognized; may have been recognized before but may potentially affect a new or different population, industry, or geographic area than previously affected; or may be an existing threat that has developed new attributes.

A House Committee report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 included a provision for us to identify emerging threats of high national security consequence.[2] This report describes long-range emerging threats as identified by DOD, State, DHS, and ODNI.[3] For purposes of this report, we define long-range threats as threats that agency officials identified that may occur in approximately 5 or more years, or those threats that could occur in a future unknown time frame.[4]

This report is a public version of a classified report that we issued on September 28, 2018.[5] It omits classified and sensitive information about threats identified by executive branch agencies and described in 26 profiles in our classified report. It also omits classified and sensitive information in those profiles related to specific threats, the effects of those threats, specific warfare domains, and questions for oversight. Although the information provided in this report is more limited, the report addresses the same objectives as the classified report and uses the same methodology.

To identify long-range emerging threats, we administered a questionnaire to 45 selected organizations across DOD, State, DHS, and ODNI.[6] In the questionnaire, we asked respondents to identify and describe emerging threats that their organizations assess could occur in approximately 5 years or more from today, or those that have an unknown time frame. We received approximately 210 individual threats from 26 of these 45

---

[1]Adversaries are potentially hostile or disruptive state or non-state actors. According to the 2018 *National Defense Strategy*, state actors and non-state actors, such as terrorists, transnational criminal organizations, and cyber hackers, have transformed the direction of global affairs with increased capabilities of mass disruption. Disruptive state actors include North Korea, Russia, China, and Iran. Non-state actors include violent extremist organizations such as al-Qaida and the Islamic State of Iraq and Syria. Transnational criminal organizations can participate in the sale of illegal drugs and counterfeit goods, human trafficking and smuggling, and other criminal activities. According to DOD officials, megacorporations are large companies that have the financial resources and a power base to exert influence on par with or exceeding non-state actors.

[2]H.R. Rep. No. 115-200, at 181 (2017).

[3]ODNI supports the Director of National Intelligence's role as head of the Intelligence Community. The Intelligence Community is comprised of 17 separate organizations such as the Central Intelligence Agency, the Defense Intelligence Agency, the Federal Bureau of Investigation, the National Security Agency, and intelligence components within agencies such as the Department of Homeland Security, Department of State, and the military services.

[4]We established this time frame because officials from DOD and ODNI stated that they consider threats occurring earlier than 5 years from today as near-term or mid-term threats, which receive greater attention and resources from defense and intelligence organizations than long-term threats.

[5]GAO, *National Security: Long-Range Emerging Threats Facing the United States Identified by Federal Agencies*, GAO-18-497SPC (Washington, D.C.: Sept. 28, 2018). (SECRET//NOFORN)

[6]We focused on DOD, State, DHS, and ODNI as among the federal agencies with primary responsibility for national security. We identified the 45 selected organizations within these agencies that assess long-range emerging threats through consultation with agency officials.

organizations, which formed the basis of our threat profiles.[7] See appendix I for more details about the specific organizations that received the questionnaire. In addition, ODNI submitted a questionnaire but did not identify any threats on the questionnaire. Instead, ODNI officials referred us to their *Global Trends: Paradox of Progress* report and provided verbal input on long-range emerging threats.[8] We used this information to supplement questionnaire responses from DOD, State, and DHS organizations. In total, we received a 78-percent response rate (28 of 36) to our questionnaire.[9]

To supplement information from the questionnaire, we reviewed documents provided by DOD, State, DHS, and ODNI. For example, we reviewed the most recent national strategies that pertain to emerging threats and ODNI's 2017 *Global Trends: Paradox of Progress* report.[10] We also interviewed officials about long-range emerging threats from 22 organizations, including 11 DOD organizations, 6 State organizations, 4 DHS organizations, and ODNI. We selected these 22 organizations because they may have a role in identifying and assessing long-range emerging threats. This review did not assess any efforts to mitigate threats. We pre-tested the questionnaire instrument with officials from different agencies to confirm that it would be understood by respondents as intended, and determined that the data collected were sufficiently reliable for our purposes.

It is not possible to predict every potential long-range emerging threat. According to Intelligence Community officials, the further out in time predictions go, the more uncertain they become, because the future is a confluence of multiple trends with an infinite number of possible permutations. For example, adversaries may use emerging technologies together in novel and unpredicted ways to amplify their harm. Several DOD officials also noted that there will always be completely unpredictable events with no prior warning. Therefore, this report does not attempt to provide a comprehensive listing of all potential emerging threats to the United States that may arise over the next 5 or more years. Rather, it represents the assessments of agency experts who responded to our questionnaire, supplemented by information from national security strategies, related agency documents, and interviews with agency officials. Furthermore, many questionnaire responses focus on threats that originate outside the United States. For more information on our objective, scope, and methodology, see appendix I.

The performance audit upon which this report is based was conducted from July 2017 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We subsequently worked with DOD from September 2018 to December 2018 to prepare this public version of the original classified report for public release. This public version was also prepared in accordance with those standards.

[7]Two additional organizations provided responses after the response period had ended. These responses were not used in the development of the threat profiles but were included in our response rate calculations.

[8]Office of the Director of National Intelligence, National Intelligence Council, *Global Trends: Paradox of Progress,* NIC 2017-001 (Washington, D.C.: January 2017). An ODNI official stated that the *Global Trends: Paradox of Progress* report lists some key threats over the next 5 to 20 years. In particular, ODNI officials emphasized economic threats such as U.S. debt and growing inequality; new technologies and ethical questions surrounding the use of those technologies; geopolitical conflict, including the spread of corruption to the developed world and the rise of China; and the spread of populism and nationalist identities around the world.

[9]Of the 45 organizations selected to receive our questionnaire, 9 organizations were excluded from our response rate calculations because 8 told us that they do not identify threats that meet our scope or definition, and 1 told us that a separate office within their organization had responded on their behalf. Of the remaining 36 organizations, 28 organizations provided responses (2 of which provided responses after the response period had ended, and were not used in the development of the threat profiles). In addition, 1 organization did not receive a questionnaire due to an administrative error and ODNI submitted an incomplete questionnaire that did not identify any threats. We did not receive responses from the remaining 6 organizations.

[10]NIC 2017-001.

Background

Current Landscape of Emerging Threats

DOD officials noted that Western liberal democratic institutions around the world are being challenged in new and novel ways. Adversaries have had over 40 years to study the United States and Western institutions. As such, the nature of warfare has evolved to include "gray zone" conflict—defined as the area between war and peace—where weaker adversaries have learned how to seize territory and advance their agendas in ways not recognized as "war" by Western democracies. Also, these gray zone conflicts can offset superior U.S. economic and security structures. DOD officials added that adversaries around the world may erode democracies, often using democratic institutions, in the gray zone of conflict.[11] ODNI officials also noted that China and Russia are pursuing gray zone strategies to achieve their objectives without resorting to military conflict.

DOD officials provided a list of recent significant examples of adversary success in the gray zone of conflict, several of which have occurred without significant consequences, including:

- Russian and Chinese near-unrestricted thefts of U.S. intellectual property, Office of Personnel Management data theft, and penetrations of U.S. civil, utility, and military data and electoral voting systems;
- Russian seizure of Ukrainian territory, namely Crimea;
- Chinese seizure of the South China Seas and the building of military islands in defiance of international court rulings;
- China using bilateral economic deals to marginalize U.S. multilateral frameworks in Asia, Africa, Latin America, and the Pacific;
- Russia attempting to resurrect former Soviet client state relationships with Syria, Egypt, and Libya, and potentially with additional countries in the Middle East and North Africa;
- Iran realigning the Middle East by using proxy forces to create friendly governments including Syria, Iraq, and Yemen at the expense of U.S. leadership in the region;
- "Strongmen" in countries such as Venezuela, Egypt, and Turkey using democratic institutions to promote new paradigms independent of Western liberal norms; and
- The continued attraction of extremist groups, including the Islamic State and al-Qaida, as a preferable means to achieve Sunni Arab autonomy as a viable alternative to minority governance in countries with majorities that outnumber them (as in Syria and Iraq).

DOD officials said that, with current demographic trends, Western liberal democratic institutions will be tested in new ways as the nature of warfare changes. The challenge for the United States and its allies will be to develop responses faster than adversaries through a better understanding of the strategic environment. Officials added that this presents a challenge since the United States appears to be strategically surprised by an evolving world.

DOD officials also said that the United States must adapt to challenges from adversaries and better link security objectives and economic objectives, or risk further erosions of U.S. influence to adversaries such as China and Russia. Officials stated that China and Russia are more agile than the United States in creating relationships with other countries to degrade U.S. bilateral and multilateral frameworks. For example, China and Russia are working to define the United States as a "status quo" power trying to preserve the old world order in what is becoming a multipolar world. These officials added that the nature of conflict has changed, and so the United States must evolve.

[11]Officials from the Defense Advanced Research Projects Agency noted that gray zone warfare is characterized by limited conflict that sits between normal state competition and what is traditionally thought of as war.

Future Landscape of Emerging Threats

ODNI's January 2017 report *Global Trends: Paradox of Progress* describes future trends that will shape the direction of the world over the next 5 or more years.[12] ODNI's report describes potential environments from which long-range threats may emerge, based on secen key global trends:

❶ **The rich population is shrinking, the poor population is not.** Working-age populations are shrinking in wealthy countries and in China and Russia, and are growing in developing, poorer countries. This trend has the potential to increase economic, employment, urbanization and welfare pressures, and spur migration.[13]

❷ **The global economy is shifting.** Weak economic growth will likely persist in the near term. Major economies will confront shrinking workforces and diminishing productivity gains while recovering from the 2008-2009 financial crises with high debt, weak demand, and doubts about globalization. Inequality and wealth concentrations—combined with corruption and eroding trust in authorities—are driving a wave of political change.

❸ **Technology is accelerating progress but causing discontinuities.** Rapid technological advancements will increase the pace of change and create new opportunities, but will aggravate divisions between winners and losers. Automation and artificial intelligence will threaten to change industries faster than economies can adjust, potentially displacing workers and limiting the usual route for poor countries to develop. Biotechnologies such as genome editing will revolutionize medicine and other fields, while sharpening moral differences.

❹ **Ideas and identities are driving a wave of exclusion.** Growing global connectivity amid weak economic growth will increase tensions within and between societies. Populism will increase on the right and the left. Some leaders will use nationalism to shore up control. Religious influence will be increasingly consequential, and nearly all countries will see economic forces boost women's status and leadership roles, but backlash against this trend also will occur.

❺ **Governing is getting harder.** The public will demand that governments deliver security and prosperity. However, flat revenues, distrust, polarization, and a growing list of emerging issues will hamper government performance. Technology will expand the range of players who can block or circumvent political action.

❻ **The nature of conflict is changing.** The risk of conflict will increase due to diverging interests among major powers, an expanding terror threat, continued instability in weak states, and the spread of lethal, disruptive technologies. Disrupting societies will become more common, with long-range precision weapons, cyber, and robotic systems to target infrastructure from afar, and with more accessible technology to create weapons of mass destruction.

❼ **Climate change, environment, and health issues will demand attention.** A range of global hazards pose imminent and longer-term threats that will require collective action to address—even as cooperation becomes harder. More extreme weather, water and soil stress, and food insecurity will disrupt societies. Sea-level rise, ocean acidification, glacial melt, and pollution will change living patterns. Tensions over climate change will grow.

The *Global Trends* report also points out that conflicts in the next 5 to 20 years will be more:

- **Diffuse**—referring to state, non-state, and sub-state entities having greater accessibility to means of warfare;
- **Diverse**—referring to the means of warfare varying across a wider spectrum, from nonmilitary capabilities to advanced conventional weapons and weapons of mass destruction; and
- **Disruptive**—referring to a greater emphasis by states and terror groups on targeting critical infrastructure, societal cohesion, and government functions, rather than defeating enemy forces on the battlefield through traditional military means.[14]

[12]NIC 2017-001.

[13]In its report, ODNI states this trend as "the rich are aging, the poor are not." See NIC 2017-001.

[14]NIC 2017-001.

Roles and Responsibilities of Agencies That Identify and Mitigate Emerging Threats

DOD, State, DHS, and the Intelligence Community have key roles in identifying and mitigating long-term emerging threats. Specifically:

- **DOD** has a role in, among other things, defending the homeland from limited ballistic missile and cruise missile attack; large-scale terrorist attack; chemical, biological, radiological, or nuclear attack; and space, electromagnetic, or kinetic attacks against our critical infrastructure. DOD also works to prevent adversaries such as state and non-state actors from acquiring, proliferating, or using weapons of mass destruction, and is the lead agency to defend U.S. military and intelligence infrastructure from cyber attacks and conduct offensive cyber operations. DOD also works to rebuild the military strength and maximize the competitive advantage of the United States and its partners, while constraining the ability of our adversaries to achieve their military objectives. DOD efforts may include preventing terrorists from directing or supporting operations against the U.S. homeland and its partners, and bolstering its partners against coercion. Finally, DOD assists State and the U.S. Agency for International Development with natural disaster and conflict response around the world.

- **State** is the lead U.S. foreign affairs agency and the lead institution for conducting American diplomacy. State plays a role in protecting and advancing the interests of the United States by, in part, countering threats and adversaries, deepening U.S. security relationships and partnerships around the world, and strengthening our allies and alliances. State also engages in security and capacity building and other non-military assistance, such as border patrol, with other countries. In conjunction with DOD and the U.S. Agency for International Development, State also responds to natural disasters and conflict-induced crises around the world.

- **DHS** plays a role in preventing a variety of threats within the homeland, particularly terrorist attacks within the United States. DHS also seeks to reduce the vulnerability of the United States to terrorism, assisting in the recovery from terrorist attacks that do occur within the United States, and disrupting connections between illegal drug trafficking and terrorism, and for coordinating efforts to sever such connections. DHS officials added that DHS is also the lead agency for defense of civilian cyber infrastructure (such as .gov accounts) from cyber-attacks, and for aiding private-sector critical-infrastructure cyber security. DHS officials also said that DHS has primary responsibility for border and transportation security issues, including interdicting illicit smuggling of humans and contraband into the homeland, traveler security screening, and, via the U.S. Coast Guard, securing the maritime approaches to the homeland.

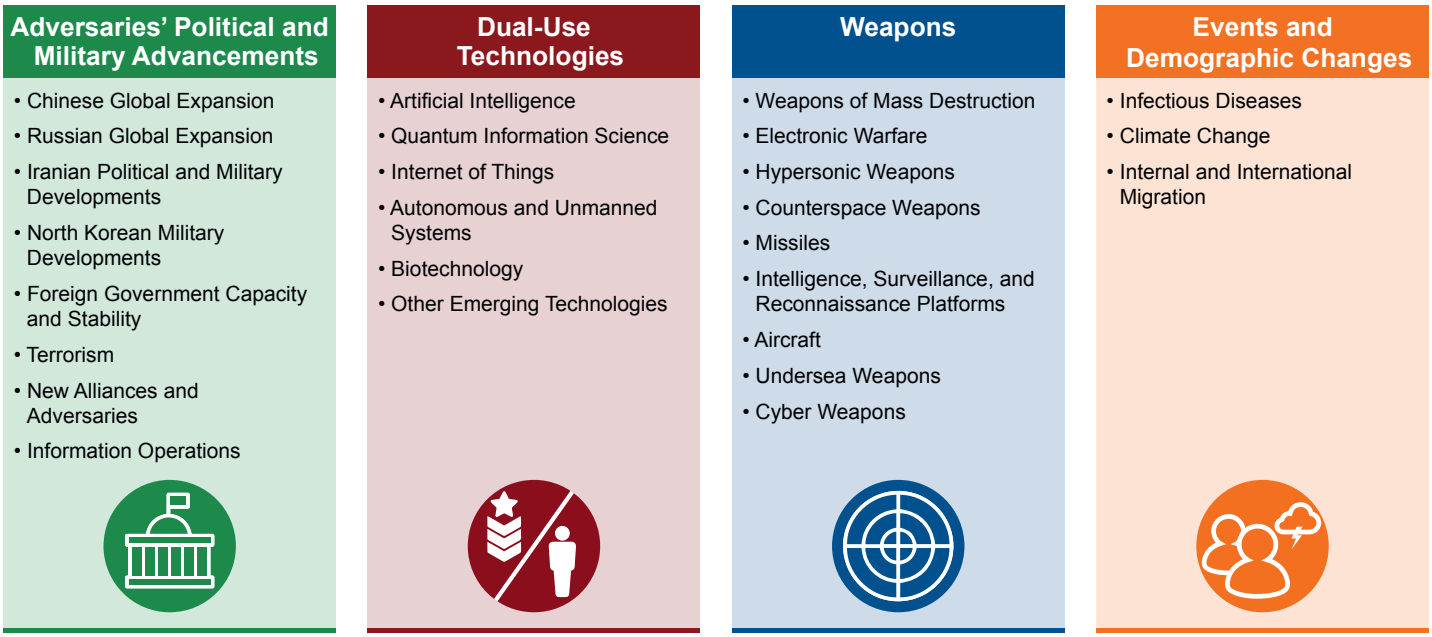
- **ODNI** supports the Director of National Intelligence in his role as the head of the Intelligence Community, acts as the principal advisor to the President, National Security Council, and the Homeland Security Council for intelligence matters related to national security, and oversees and directs the implementation of the National Intelligence Program.[15] ODNI's activities include integrating intelligence analysis and collection, driving secure information sharing, setting strategic direction and priorities for national intelligence resources and capabilities, developing and implementing unifying intelligence strategies, and advancing capabilities to provide the United States with a global intelligence advantage.

[15]The National Intelligence Program is intended to provide the resources to develop and maintain intelligence capabilities that support national priorities. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1011 (2004). According to 50 U.S.C. § 3003 (6) "the term 'National Intelligence Program' refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of National Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces."

DOD, State, DHS and ODNI Identified a Variety of Emerging Threats to U.S. National Security That May Occur over the Next Approximately 5 or More Years

DOD, State, DHS, and ODNI independently identified various emerging threats to the United States or its national security interests. Our analysis of these threats led to 26 threat profiles that fell within four broad categories: 1) Adversaries' Political and Military Advancements, 2) Dual-Use Technologies, 3) Weapons, and 4) Events and Demographic Changes, as shown in figure 1.

Figure 1: GAO's Four Broad Categories for 26 Long-Range Emerging Threats Identified by DOD, State, DHS, and ODNI



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

Adversaries' Political and Military Advancements »

Our adversaries are developing new political and military policies, strategies, doctrines, and tactics to advance their interests. These activities may or may not be intended to harm the United States and its national security interests. Agency officials identified examples such as Russia's integration of irregular warfare, influence operations, deception, and cyber attacks. Figure 2 shows the identified threats for this category.

Figure 2: Threats Identified under Adversaries' Political and Military Advancements

Threat »	Description »	Examples »
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.	• Expansion and Power Projection • Fusion of Military and Civilian Sectors and Control of Supply Chain • Cyber and Electronic Warfare
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.	• Military Capabilities across Warfare Domains • Global Military and Political Influence • Biotechnology Advancements
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.	• Military and Economic Influence • Ballistic Missiles • Cyber Attacks
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.	• Nuclear Strike against the Continental United States • Numerical Overmatch of Ballistic Missile Systems
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.	• Governments' Ability to Address Influences from Violent Extremist Organizations • Foreign Militaries' Reduced Military Readiness • Instability in Africa • Instability in Latin America and the Caribbean
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.	• Proliferation of Terrorism and Violent Ideologies • Terrorist Use of Chemical, Biological, and Nuclear Materials • New Tactics and Techniques
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).	• Disrupted Alliances • Rise of New Nation-State and Non-State Adversaries • Foreign Nation-States' Influences on International Agreements and Standards
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.	• Exploitation and Theft of U.S. Information • Weaponized Information

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

Dual-Use Technologies »

These are technologies that may be developed by governments or the private sector for benign or beneficial purposes, but may have a dual-use application. For instance, in an adversary's hands, these technologies may pose a risk to the United States. Agency officials identified examples such as unmanned vehicles, artificial intelligence, and encryption technologies. Figure 3 shows the identified threats for this category.

Figure 3: Threats Identified under Dual-Use Technologies

Threat »	Description »	Examples »
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.	• Nation-State and Non-State Development of AI • Intelligent Systems with General AI
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.	• Quantum Communications • Quantum Computing
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.	• Unsecure Networks and Data • Attacks on IoT-Enabled Infrastructure • Attacks on Commercial and Military 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.	• Enhancement of Autonomous Systems • Weapons with Autonomous Navigation • Autonomous and Unmanned Vehicles
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.	• Human Genetic Modification and Synthetic Biology • Plant and Animal Genetic Modification • Other Biotechnology Applications • Increase Access to Technology
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.	• Expansion of Removable Media and Storage • Additive Manufacturing • New Materials • Development of Technologies that Address Electric Power Scarcity • Advancements in Camouflage Technology • Advanced Sensors

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

Weapons »

These threats are inherently threatening military devices that may be used by our adversaries to inflict harm upon the United States or its national security interests. These weapons do not have potential beneficial or benign uses from the perspective of the United States. Agency officials identified examples such as hypersonic missiles, weaponized pathogens, or stealth aircraft. Figure 4 shows the identified threats for this category.

Figure 4: Threats Identified under Weapons

Threat »	Description »	Examples »
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.	• Global Proliferation of Weapons of Mass Destruction • Development and Use of Nonstrategic Nuclear Weapons • New Forms of Biological Weapons
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.	• Electronic Attack Weapons • Attacks on Communications and Navigation Systems
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.	• Hypersonic Weapons and Missile Defense • Hypersonic Ballistic and Cruise Missiles • Hypersonic Glide Vehicles • Future Development and Convergence
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.	• Anti-Satellite Weapons • Increased Access to Space and Anti-Satellite Weapons
Missiles	Adversaries are developing missile technology to attack the United States in novel ways and challenge U.S. missile defense, including conventional and nuclear intercontinental ballistic missiles, sea-launched land-attack missiles, and space-based missiles that could orbit the earth.	• Advancements in Missile Technology • Adversary Plans for Intercontinental Ballistic Missiles • Orbital Missiles • Sea-to-Land Missiles • Adversary Missile Defense
Intelligence, Surveillance, Reconnaissance (ISR) Platforms	Future advances in artificial intelligence, 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.	• Worldwide and Ubiquitous Surveillance • Adversary Improvements in Radar and Surveillance 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.	• Russian Aircraft • Chinese Aircraft
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 artificial intelligence to locate U.S. submarines—or attack U.S. undersea infrastructure, which could cripple communications.	• Russian Improvements in Undersea Stealth • Unmanned Underwater Vehicles • Anti-Submarine Warfare • Attack on Undersea Cables
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.	• Attacks on Critical Infrastructure • Military Infrastructure • Cyber Attacks on Health Care • Malware and New Form of Attack

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

Events and Demographic Changes »

Events and demographic changes are occurrences with no adversary behind them and therefore no intent to harm the United States. Nevertheless, events and demographic changes may have the capability to harm the United States or its national security interests in the absence of mitigating factors. Agency officials identified examples such as influenza pandemic, climate change, food shortages, and the growth of megacities. Figure 4 shows the identified threats for this category.

Figure 5: Threats Identified under Events and Demographic Changes

Threat »	Description »	Examples »
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.	• Pandemic Disease Event • Drug-Resistant Disease
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.	• Extreme Weather Events • Loss of Arctic Sea Ice and Permafrost
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.	• Disasters in Megacities • A Mass Migration Event

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

Agency Comments and Our Evaluation

We provided a draft of the classified version of this report to the DOD, State, and DHS, as well as ODNI, for their review and comment. DOD concurred with our classified report and provided technical comments, which we addressed as appropriate. DOD's letter is included in appendix II. We also received technical comments from DHS and ODNI, which we addressed as appropriate. State did not provide comments.

We are sending copies of this report to the appropriate congressional committees, DOD, State, DHS, and ODNI. In addition, this report is available at no charge on the GAO website at www.gao.gov.

If you have any questions about this report or need additional information, please contact Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov, or Brian M. Mazanec at (202) 512-5130 or MazanecB@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last pages of this report.

In addition to the individuals named above, Tommy Baril and Hynek Kalkus (Assistant Directors), Heather Salinas (Analyst-in-Charge), Ben Emmel, Jamilah Moon, Katya Rodriguez, and Spencer Tacktill made key contributions to this report. Tracy Barnes, Amie Lesser, Amanda Miller, Richard Powelson, Michael Silver, and Alexander Welsh also provided contributions.

Joseph W. Kirschbaum
Director
Defense Capabilities and Management

Brian M. Mazanec
Acting Director
International Affairs and Trade

List of Congressional Committees

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

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

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

The Honorable Kay Granger
Chairwoman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objective, Scope, and Methodology

This report is a public version of a classified report that we issued on September 28, 2018.[1] It omits classified and sensitive information about threats identified by executive branch agencies and described in 26 profiles in our classified report. It also omits classified and sensitive information in those profiles related to specific threats, the effects of those threats, specific warfare domains, and questions for oversight. Although the information provided in this report is more limited, the report addresses the same objectives as the classified report and uses the same methodology.

This report provides a summary of long-range emerging threats as identified by agencies that, among others, have primary responsibility for national security: the Department of Defense (DOD), Department of State (State), Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI). We utilized questionnaires, national security strategies, agency documents, and interviews with agency officials to obtain information on these long-range emerging threats. For purposes of this report, we define long-range threats as threats that agency officials identified that may occur in approximately 5 or more years, or those threats that could occur in a future unknown time frame.

There is no standard definition of "emerging threat" within the federal government, and the use and definitions of the term vary among organizations. To develop a definition of emerging threat that generally reflected how multiple organizations use this term, we reviewed strategies and reports issued by federal government entities—such as the 2016 *Joint Strategic Intelligence Estimate* from the Joint Staff and *Global Trends: Paradox of Progress* from the National Intelligence Council—that describe issues, risks, threats, or events that could affect the national security interests of the United States and its allies. We also reviewed documents such as the *DOD Dictionary of Military and Associated Terms and the Department of Homeland Security Risk Assessment Lexicon* that define and standardize commonly-used terminology. We reviewed our past reports and publications by research institutions to understand how different organizations consider and utilize the concepts of "emergence" and "threat." We adapted the use of the term "emerging" from our prior work in emerging infectious diseases, and adapted the use of the term "threat" from the documents we reviewed.[2]

After developing a working definition of emerging threat, we solicited feedback on the definition through interviews with officials from DOD, State, and ODNI, including assessing whether the definition would be acceptable or understood within their respective organizations. We modified the definition based on their feedback. Furthermore, we limited the scope of emerging threats, as described in this report, to threats that may occur approximately 5 years or more from 2018, or those that have an unknown time frame. We established this time frame because officials from DOD and ODNI stated they consider threats occurring earlier than 5 years from today as near-term or mid-term threats, which receive greater attention and resources from defense and intelligence organizations than long-term threats.

As the primary mechanism for identifying emerging threats within our identified time frame, we developed a questionnaire that asked respondents to identify and describe emerging threats that their organizations assess could occur in approximately 5 years or more from today, or those that have an unknown time frame. To identify organizations within DOD, State, DHS, and the Intelligence Community to receive this questionnaire, we consulted with officials from DOD, State, DHS, and ODNI about the objective, scope, and methodology of our work. We then identified additional organizations through an iterative process whereby we contacted DOD, State, DHS and ODNI officials and solicited the names of additional organizations that assess emerging threats. We repeated this process until the referrals were mostly to organizations we had previously contacted.

[1]GAO, *National Security: Long-Range Emerging Threats Facing the United States Identified by Federal Agencies*, GAO-18-497SPC (Washington, D.C.: Sept. 28, 2018). (SECRET//NOFORN)

[2]GAO, *Emerging Infectious Diseases: Actions Needed to Address the Challenges of Responding to Zika Virus Disease Outbreaks*, GAO-17-445 (Washington, D.C.: May 23, 2017).

Ultimately, we selected a total of 45 organizations to receive the questionnaire, comprised of 36 organizations identified through the iterative process described previously and the nine combatant commands.[3] We took several steps to ensure that the questionnaire would gather reliable information. The questionnaire was developed in collaboration with a survey specialist and was reviewed by a separate survey specialist. We requested and received comments from subject matter experts from DOD, State, and DHS. We also conducted six pretests of the questionnaire with potential recipients to assess how the questionnaire would be understood by the eventual recipients. The pretest participants included officials from each department requested to respond to the questionnaire (DOD, State, and DHS) who had not previously reviewed or provided comments on the questionnaire. We refined the questionnaire based on the results of each step. Additionally, we included an example to guide respondents to the type and length of content we wanted them to provide in their response. The final questionnaire was a Microsoft Word form that the respondents could return electronically.

Out of the 45 government organizations selected, 8 told us that they do not identify threats that meet our scope or definition, and 1 told us that a separate office within their organization had responded on their behalf, so these 9 organizations were excluded from our response rate calculations. Of the remaining 36 organizations, 26 provided responses by the end of the response period and 2 provided responses after the response period had ended so they were not used in the development of the threat profiles.[4] In addition, 1 organization did not receive a questionnaire due to an administrative error and ODNI submitted an incomplete questionnaire that did not identify any threats. Instead, ODNI referred us to their Global Trends: Paradox of Progress report and provided verbal input on long-range emerging threats during two agency meetings.[5] We used this information to supplement questionnaire responses from DOD, State, and DHS organizations. We did not receive responses from the remaining six organizations. In total, we received a 78-percent response rate (28 of 36) of organizations that provided completed questionnaire responses. Table 1 lists the 28 organizations that provided completed responses to our questionnaire.

[3]U.S. Cyber Command was elevated to a combatant command on May 5, 2018—after we sent the questionnaire. Therefore, U.S. Cyber Command was not included among the combatant commands that received a questionnaire.

[4]These responses were submitted more than 3 months after the submission deadline. Many of these responses were similar to previously submitted questionnaire responses, but some of the emerging threats were different.

[5]An ODNI official stated that the *Global Trends: Paradox of Progress* report lists some key threats over the next 5 to 20 years. In particular, ODNI officials emphasized economic threats such as U.S. debt and growing inequality; new technologies and ethical questions surrounding the use of those technologies; geopolitical conflict, including the spread of corruption to the developed world and the rise of China; and the spread of populism and nationalist identities around the world.

Table 1: Organizations That Provided Completed Questionnaire Responses

Department of Defense	Department of State	Department of Homeland Security
Office of Assistant Secretary for Research and Engineering, Office of Net Technical Assessment	Bureau of Oceans and International Environment and Scientific Affairs	Countering Weapons of Mass Destruction Office
Office of Assistant Secretary for Research and Engineering, Deputy Assistant Secretary of Defense, Emerging Capabilities and Prototyping	Office of Medical Services, Directorate of Operational Medicine	Office of Science and Technology
Strategic Capabilities Office		Office of Intelligence and Analysis[a]
Office of Net Assessment		Federal Emergency Management Agency
Defense Advanced Research Projects Agency[a]		National Protection and Programs Directorate
Defense Intelligence Agency, Office for Space and Counterspace		
Defense Intelligence Agency, Defense Technology and Long Range Analysis		
Defense Intelligence Agency, National Center for Medical Intelligence		
National Security Agency		
U.S. Army, National Ground Intelligence Center		
U.S. Navy, Acquisition, Intelligence, and Requirements Office		
U.S. Air Force, National Air and Space Intelligence Center		
U.S. Marine Corps, Marine Corps Intelligence Activity		
U.S. Africa Command		
U.S. European Command		
U.S. Northern Command		
U.S. Indo-Pacific Command		
U.S. Southern Command		
U.S. Special Operations Command		
U.S. Strategic Command		
U.S. Transportation Command		

Source: GAO. | GAO-19-204SP

[a]Defense Advanced Research Projects Agency and the Department of Homeland Security's Office of Intelligence and Analysis submitted completed questionnaires after our response period had ended. The information received in these questionnaires was not used in the development of the threat profiles.

The 26 of 28 organizations that timely responded provided approximately 210 individual threats, 4 of which were later deemed outside of the scope of this review. The questionnaire responses are not generalizable to any other organizations.

We then conducted a content analysis of the questionnaire responses to categorize threats and to identify common themes across responding organizations. Two analysts independently reviewed and coded each threat described in the questionnaires according to the categorization framework. After all of the individual threats had been coded, the analysts met, discussed any differences, and reached agreement on the final coding for each individual threat. A third analyst adjudicated any unresolved differences between coders.

To consistently report on all emerging threats identified during this review, the analysts conducted a second phase of content analysis. Using primarily the list of descriptors and the threats coded to each descriptor, three analysts developed a list of 26 threats described in separate profiles in this report. In this process, some descriptors were combined into a single threat profile, while others were renamed to more accurately reflect the threats associated with the descriptor and threat profile. The analysts coded each of the approximately 210 individual threats into 1 of the 26 threat profiles. The analysts resolved any differences by discussion and consensus. We also reviewed documents provided by organizations that participated in this review to determine whether the documents identified emerging threats differently from those identified through the questionnaire responses and content analysis. We did not identify any additional emerging threats through this document review.

We also used information in related documents—such as a DOD risk assessment, DOD threat reports, GAO reports, a Defense Science Board report, National Academy of Sciences reports, and National Intelligence Council reports—to supplement the information gathered from the processes listed above.

To supplement the questionnaire responses and our review of the national security strategies and other documents, we interviewed officials from DOD, State, DHS, and ODNI. In total, we interviewed officials from 22 organizations, including 11 DOD organizations such as the Defense Intelligence Agency, several combatant commands, and the Joint Staff; 6 State organizations across 5 bureaus, including the Bureaus of Counterterrorism and Countering Violent Extremism, Intelligence and Research, and Oceans and International Environmental and Scientific Affairs; 4 DHS organizations, such as the Science and Technology Directorate and the Countering Weapons of Mass Destruction Office; and ODNI. We selected these 22 organizations because they may have a role in identifying and assessing long-range emerging threats. Additionally, we interviewed officials at the headquarters of the North Atlantic Treaty Organization, U.S. Africa Command, and U.S. European Command. We selected these sites because officials within DOD and State identified these organizations as representative military commands that identify and address emerging threats.

The performance audit upon which this report is based was conducted from July 2017 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from September 2018 to December 2018 to prepare this public version of the original classified report for public release. This public version was also prepared in accordance with those standards.

Appendix II: DOD Comments

We received these comments on September 25, 2018. The draft report number for the classified version of this report, GAO-18-497C, was subsequently renumbered GAO-18-497SPC for the final classified report.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

MEMORANDUM FOR MR. JOSEPH KIRSCHBAUM, DIRECTOR, DEFENSE CAPABILITIES MANAGEMENT, U.S.GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: Review of GAO Draft Report

Reference: GAO Draft Report, GAO-18-497C, "NATIONAL SECURITY: Long-Range Emerging Threats Facing the United States Identified by Federal Agencies, dated July 26, 2018 (GAO Code 102221)

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-18-497, "NATIONAL SECURITY: Long-Range Emerging Threats Facing the United States Identified by Federal Agencies, dated July 26, 2018 (GAO Code 102221). The Department appreciates the opportunity to review and comment on the draft report. We concur with the report as a whole with some recommendations.

The security review determined that the overall classification of the report must remain SECRET//NOFORN, except as indicated when separated from the report. Paragraphs have been portioned marked in accordance with security guidelines.

Overall, we find this GAO study of high quality while providing an accurate although sobering macro picture of how the US stands in the world against emerging threats.

My point of contact for this effort is Mr. Rich Matthews, 703-697-8743, richard.e.matthews18.civ@mail.smil.mil in the Office of the Under Secretary of Defense (Intelligence), Director for Defense Intelligence, Warfighter Support Division, (703) 697-8743.

Wendell C. Warner, DISES
Director, Geographic Combatant Command
Intelligence Support

(U) Related GAO Products

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD. GAO-17-668. Washington, D.C.: July 27, 2017.

Infectious Disease Threats: Funding and Performance of Key Preparedness and Capacity-Building Programs. GAO-18-362. Washington, D.C.: May 24, 2018

Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications. GAO-18-142SP. Washington, D.C.: March 28, 2018.

Trends Affecting Government and Society: United States Government Accountability Office Strategic Plan 2018-2023. GAO-18-396SP. Washington, D.C.: February 22, 2018.

Tax Fraud and Noncompliance: IRS Can Strengthen Pre-refund Verification and Explore More Uses. GAO-18-224. Washington, D.C.: January 30, 2018.

Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. GAO-18-177. Washington, D.C.: January 18, 2018.

Nuclear Security: CBP Needs to Take Action to Ensure Imported Radiological Material Is Properly Licensed. GAO-18-214. Washington, D.C.: January 10, 2018.

Climate Change Adaptation: DOD Needs to Better Incorporate Adaptation into Planning and Collaboration at Overseas Installations. GAO-18-206. Washington, D.C.: November 13, 2017.

Identity Theft: Improved Collaboration Could Increase Success of IRS Initiatives to Prevent Refund Fraud. GAO-18-20. Washington, D.C.: November 28, 2017.

Diplomatic Security: Key Oversight Issues. GAO-17-681SP. Washington, D.C.: September 7, 2017.

Countering ISIS and Its Effects: Key Issues for Oversight. GAO-17-687SP. Washington, D.C.: July 18, 2017.

Emerging Infectious Diseases: Actions Needed to Address the Challenges of Responding to Zika Virus Disease Outbreaks. GAO-17-445. Washington, D.C.: May 23, 2017.

Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World. GAO-17-75. Washington, D.C.: May 15, 2017.

Russia: U.S. Government Takes a Country-Specific Approach to Addressing Disinformation Overseas. GAO-17-382C. Washington, D.C.: May 2, 2017. (SECRET//NOFORN)

Countering ISIS and Its Effects: Key Oversight Issues. GAO-17-354SPC. Washington, D.C.: April 20, 2017. (SECRET//NOFORN)

Avian Influenza: USDA Has Taken Actions to Reduce Risks but Needs a Plan to Evaluate Its Efforts. GAO-17-360. Washington, D.C.: April 13, 2017.

Nuclear Security: DOE Could Improve Aspects of Nuclear Security Reporting. GAO-17-239. Washington, D.C.: April 11, 2017.

Radioactive Sources: Opportunities Exist for Federal Agencies to Strengthen Transportation Security. GAO-17-58. Washington, D.C.: February 7, 2017.

Combating Terrorism: Additional Steps Needed in U.S. Efforts to Counter ISIS Messaging. GAO-17-41C. Washington, D.C.: December 8, 2016. (SECRET//NOFORN)

Nuclear Security: NRC Has Enhanced the Controls of Dangerous Radioactive Materials, but Vulnerabilities Remain. GAO-16-330. Washington, D.C.: July 1, 2016.

Identity Theft and Tax Fraud: IRS Needs to Update its Risk Assessment for the Taxpayer Protection Program. GAO-16-508. Washington, D.C.: May 24, 2016.

Combatting Nuclear Smuggling: NNSA's Detection and Deterrence Program is Addressing Challenges but Should Improve Its Program Plan. GAO-16-460. Washington, D.C.: June 17, 2016.

Iran Nuclear Agreement: The International Atomic Energy Agency's Authorities, Resources, and Challenges. GAO-16-565. Washington, D.C.: June 9, 2016.

Emerging Infectious Diseases: Preliminary Observations on the Zika Virus Outbreak. GAO-16-470T. Washington, D.C.: March 2, 2016.

Emerging Animal Diseases: Actions Needed to Better Position USDA to Address Future Risks. GAO-16-132. Washington, D.C.: December 15, 2015.

Nuclear Nonproliferation: NNSA's Threat Assessment Process Could Be Improved. GAO-16-118. Washington, D.C.: October 30, 2015.

Nuclear Nonproliferation: DOE Made Progress to Secure Vulnerable Nuclear Materials Worldwide, but Opportunities Exist to Improve Its Efforts. GAO-15-799. Washington, D.C.: September 23, 2015.

Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning. GAO-15-749. Washington, D.C. July 23, 2015.

Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks and Estimate of Costs, Benefits and Risks. GAO-15-119. Washington, D.C.: January 20, 2015.

Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud. GAO-14-633. Washington, D.C.: August 20, 2014.

Climate Change: Future Federal Adaptation Efforts Could Better Support Local Infrastructure Decision Makers. GAO-13-242. Washington, D.C.: May 14, 2013.

(103090)

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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

Please Print on Recycled Paper.