



Information Environment

Opportunities and Threats to DOD's National Security Mission

September 2022

GAO-22-104714

Report to Congressional Addressees

Information Environment

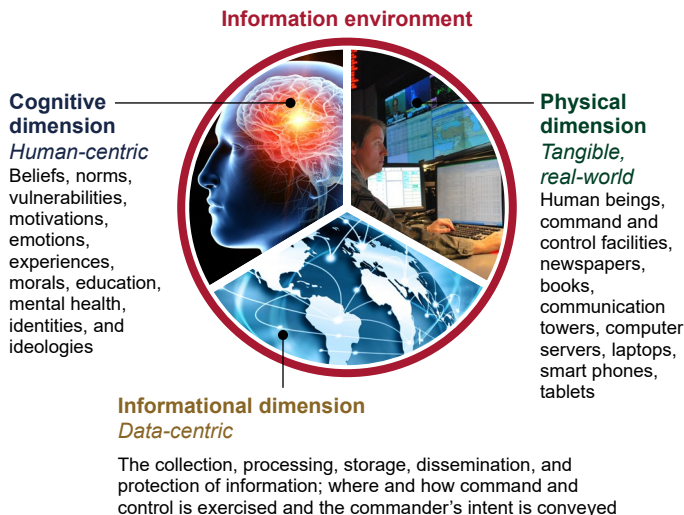
Opportunities and Threats to DOD's National Security Mission

Why GAO Did This Study

Today's information environment poses new and complex challenges for national security as the world has shifted from an industrial age to an information age. Advances in information technology, wireless communications, and social media have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. The United States' competitors and adversaries are taking advantage of these advances and the subsequent effects in the information environment to offset the U.S.'s conventional warfighting advantages.

The Department of Defense (DOD) defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information—consisting of physical, informational, and cognitive dimensions, as shown in the figure below.

Three Dimensions of the Information Environment



Source: GAO analysis of Department of Defense information; U.S. Air Force/Capt. Justin Brockhoff, Victoria/stock.adobe.com, and SciePro/stock.adobe.com (photos). | GAO-22-104714

To illustrate and better inform Congress and DOD officials, this report describes DOD's use and protection of the information environment through the following six key elements—ubiquitous and malign information, effects on DOD's mission, threat actors, threat actions, institutional challenges, and emerging technologies that can enable or adversely affect DOD's missions. This report also describes DOD actions taken and planned to use and protect the information environment.

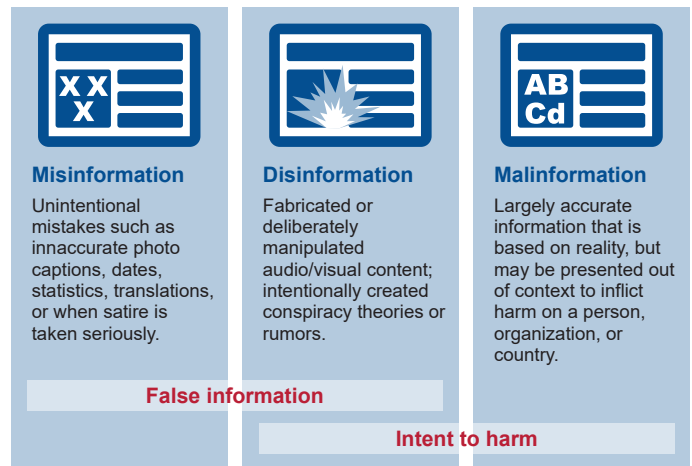
To prepare this report, among other things, GAO administered questionnaires to 25 DOD organizations involved in the information environment. GAO staff also interviewed officials and subject matter experts; reviewed 35 documents on strategy, policy, doctrine, and other guidance from DOD and other federal agencies; and reviewed studies and other documents.

What GAO Found

Given the ubiquitous nature of the information environment, both DOD and adversaries can conduct operations and activities in the information environment from anywhere in the world. Additionally, with DOD capabilities dependent on IT and the electromagnetic spectrum (EMS), its ability to conduct operations and activities in any of the physical domains (land, maritime, air, and space) is reliant on protecting the information environment. Based on a review of DOD strategies, questionnaires, interviews, and guidance documents, GAO found:

Ubiquitous and Malign Information. The fusion of ubiquitous information and technology has granted individuals, organizations, and nation-states the ability to target the cognitive foundations of individuals—beliefs, emotions, and experiences—for purposes either benign or malign. The proliferation of ubiquitous information, misinformation, disinformation, and malinformation has prompted defense experts to begin examining the concept of cognitive security.

Relationship between Misinformation, Disinformation, and Malinformation



Source: GAO analysis of Department of Homeland Security information. | GAO-22-104714

DOD Missions and Functions. Technology, the EMS, and the sharing of data are integral to accomplishing DOD's missions in the information environment. DOD components consistently identified the conduct of military operations, communications, command and control decision-making, and others, as missions and functions affected by the information environment.

Threat Actors. National and DOD strategies recognize that nation-states—such as China, Russia, Iran, and North Korea—have demonstrated that they are threat actors in the information environment, employing malicious cyber, EMS, and influence activities against DOD interests. Additionally, non-state actors—such as insider threats, foreign terrorists, transnational criminal organizations, and others—pose a threat to DOD personnel at home and abroad.

Threat Actions. DOD components highlighted a variety of cyberspace threats, information or intelligence collection threats, influence threats, and EMS threats that adversely affect DOD personnel and capabilities (see figure below).

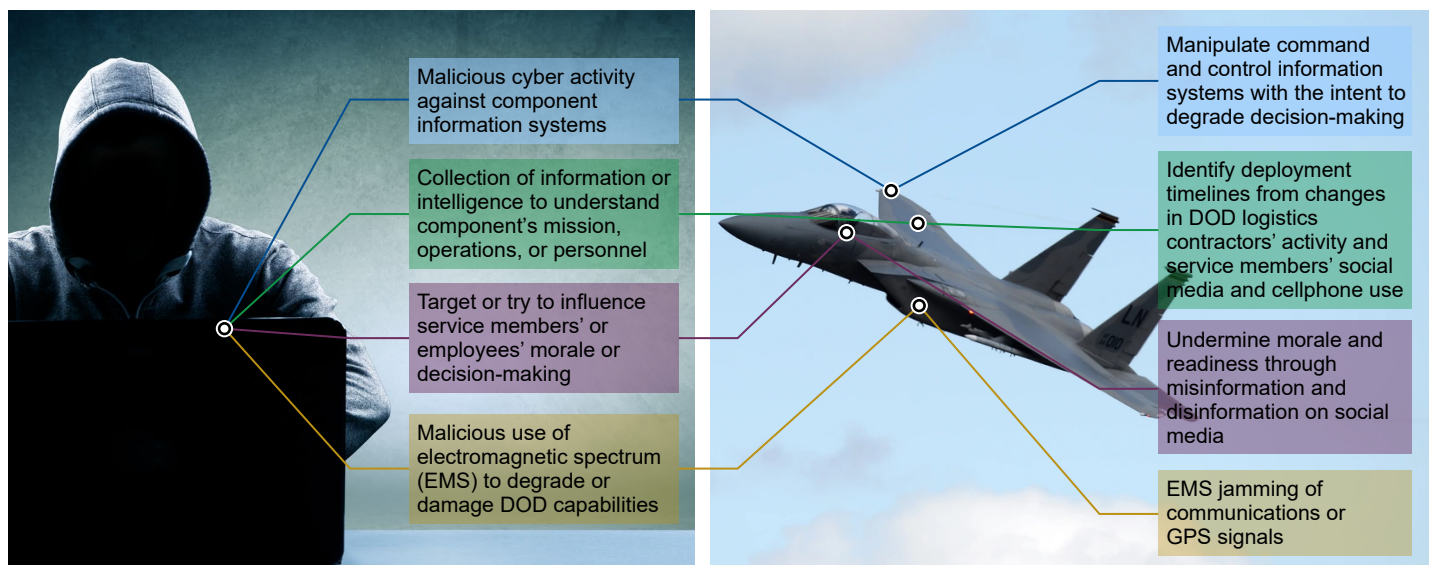
Institutional Challenges. National and DOD strategies and documents identify a number of institutional challenges that DOD must address. The challenges include a lack of leadership emphasis, lack of resources, the implications of new technologies, and dated processes. DOD components identified personnel, funding, IT, organization, and training as the most important institutional challenges they face related to the information environment.

Emerging Technologies. DOD components identified a variety of technologies that may present either opportunities for or threats to DOD in the information environment: artificial intelligence and machine learning, quantum computing, social media platforms, and bots. Additionally, relevant reports and subject matter experts have identified extended reality, fifth-generation wireless telecommunications, and the Internet of Things as technologies that could have either positive benefits or negative consequences for DOD.

Past and Planned DOD Actions. Achieving and sustaining an advantage requires DOD to undertake and plan actions across multiple areas, including doctrine, organization, and training. For example, DOD elevated the concept of “information” and has been revising its doctrine publications to reflect the fundamental nature of information in joint operations.

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

Threat Actions in the Information Environment



Source: GAO analysis of Department of Defense (DOD) information; Thaut Images/stock.adobe.com and U.S. Air Force/Staff Sgt. E. Nuñez (photos). | GAO-22-104714



Contents

| | |
|--|----|
| Letter | 1 |
| Ubiquitous and Malign Information | 6 |
| Missions and Functions Affected by Operations in the Information Environment | 9 |
| Threat Actors Associated with the Information Environment | 13 |
| Threat Actions Associated with the Information Environment | 17 |
| Institutional Challenges for DOD Related to the Information Environment | 21 |
| Emerging Technologies Associated with the Information Environment | 24 |
| Past and Planned Actions to Use or Protect the Information Environment | 30 |
| Agency Comments and Our Evaluation | 33 |
| Appendix I | 35 |
| Evolution of Information as a Joint Function and Operations in the Information Environment | |
| Appendix II | 39 |
| Objectives, Scope, and Methodology | |
| Appendix III | 42 |
| Questionnaire Administered to DOD Components | |
| Appendix IV | 52 |
| DOD Comments | |
| Related GAO Products | 53 |

This is a work of the U.S. government and is not subject to copyright protection in the United States.

The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



Abbreviations

| | |
|-----------|---|
| 5G | fifth-generation wireless technologies |
| AFRICOM | U.S. Africa Command |
| AI | artificial intelligence |
| EMS | electromagnetic spectrum |
| DARPA | Defense Advanced Research Projects Agency |
| DDS | Defense Digital Service |
| DISA | Defense Information Systems Agency |
| DIA | Defense Intelligence Agency |
| DMA | Defense Media Activity |
| DOD | Department of Defense |
| INDOPACOM | U.S. Indo-Pacific Command |
| IoT | Internet of Things |
| IT | information technology |
| JIOWC | Joint Information Operations Warfare Center |
| NORTHCOM | U.S. Northern Command |
| NSA | National Security Agency |
| SOUTHCOM | U.S. Southern Command |
| SPACECOM | U.S. Space Command |
| STRATCOM | U.S. Strategic Command |
| TRANSCOM | U.S. Transportation Command |

September 21, 2022

Congressional Addressees

Today's information environment poses new and complex challenges for national security. As we have shifted from an industrial age to an information age, advances in information technology (IT), wireless communications, and social media have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. Our competitors and adversaries are taking advantage of advances in IT, and the subsequent effects in the information environment, to offset the United States' conventional warfighting advantages.

The Department of Defense (DOD) defines the information environment—the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information—as consisting of physical, informational, and cognitive dimensions.¹ These dimensions continuously interact with individuals, organizations, and systems as shown in figure 1.

A notional example of this would be a commander using a laptop (physical dimension) to send an encrypted message (informational dimension) to a subordinate who, upon reading the message, makes a decision and acts upon the information contained in the message (cognitive dimension).

Another example would be when an adversary posts inaccurate information on social media (informational dimension) and DOD personnel reading this information on their personal devices (physical dimension) believe the inaccurate information and become frustrated or lose confidence in their commander(s), national leaders, or both (cognitive dimension). In military information operations—whether below the threshold of armed conflict or in combat activities—the ultimate goal is to influence or defeat the adversary psychologically. Achieving effects in the cognitive dimension can be a decisive step toward this goal. However, as noted by Army doctrine, the cognitive dimension is the hardest to understand.²

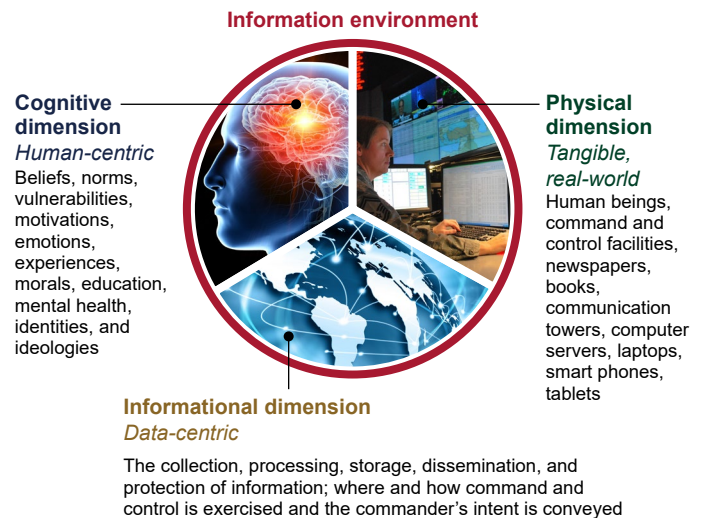
¹Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014). In a forthcoming draft Joint Publication that we reviewed, DOD reframes the information environment *dimensions* into physical, informational, and human *aspects*. More description of the draft Joint Publication can be found in appendix I.

²Department of the Army, *The Conduct of Information Operations*, ATP 3-13.1 (October 2018).

³This could occur through implanting, manipulating, extracting, or deleting data in IT systems or interfering with the operation of EMS-dependent systems.

⁴Misinformation is characterized by unintentional mistakes such as inaccurate photo captions, dates, statistics, translations, or when satire is taken seriously. Disinformation is fabricated or deliberately manipulated content, such as intentionally created conspiracy theories or rumors. Malinformation is information that is based on fact, but used out of context to mislead, harm, or manipulate a person, organization, or country. For additional discussions of these concepts, see the profile sheet on Ubiquitous and Malign Information.

Figure 1: Three Dimensions of the Information Environment



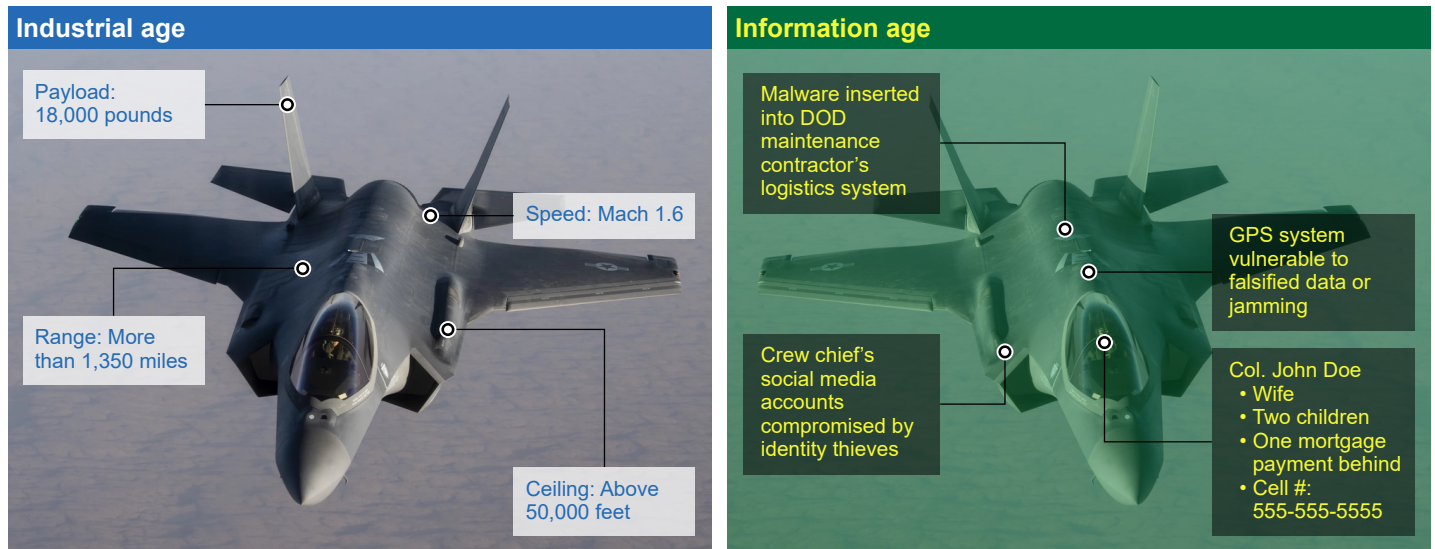
Source: GAO analysis of Department of Defense information; U.S. Air Force/Capt. Justin Brockhoff, Victoria/stock.adobe.com, and SciePro/stock.adobe.com (photos). | GAO-22-104714

Note: In a forthcoming draft Joint Publication that we reviewed, DOD reframes the information environment *dimensions* into physical, informational, and human *aspects*. More description of the draft Joint Publication can be found in appendix I.

An adversary can undermine DOD's ability to achieve its overall mission to defend and protect the United States—including its operational and tactical goals—through activities in the information environment. Such activities could include:

- Undermining the confidentiality, integrity, and availability of *information* transiting IT systems or the electromagnetic spectrum (EMS).³
- Degrading IT or EMS *systems* embedded in DOD capabilities in the physical domains (land, air, maritime, and space).
- Manipulating *decisions* made by service members, employees, contractors, dependents, and leaders. This could occur through misinformation, disinformation, or malinformation.⁴ It could also occur by exploiting people's biases.

Figure 2: Juxtaposition of Industrial-Age Capabilities versus Information-Age Vulnerabilities



Source: GAO analysis of Department of Defense information; U.S. Air Force/Airman 1st Class D. Bevan (photo). | GAO-22-104714

These information-age activities allow adversaries to target our capabilities and adversely affect military business functions and missions in ways that offset the industrial-age advantages we have developed, as shown in figure 2.

As a result of these activities, DOD must continue to find ways to protect information, systems, and minds through disparate security fields, such as information security, operations security, cybersecurity, physical security, and cognitive security.⁵

Given the ubiquitous nature of the information environment (i.e., ability to access, analyze, and leverage data from anywhere), both DOD and adversaries can conduct operations and activities in the information environment from any place on the globe. Additionally, with DOD capabilities dependent on IT and the EMS, our ability to conduct operations and activities in any of the physical domains is reliant on protecting the information environment, as illustrated in figure 3.

The ability of the United States and our allies and partners to use and protect the information environment is critical because all instruments of national power—including diplomacy, information, military, economics, financial, intelligence, and law enforcement—rely on the information environment. As noted in DOD’s *Joint Concept for Operating in the Information Environment*, IT has significantly elevated the importance of information as an instrument of power in politics, economics, and warfare.⁶ Further, since our adversaries can achieve strategic,

operational, and tactical goals below the threshold of armed conflict through the information environment, we can expect them to continue to engage us in this battlespace with the intention of eroding our national security for the foreseeable future.

In 2017, DOD updated its *Doctrine for the Armed Forces of the United States* to establish information as the seventh joint function of the military, along with the joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.⁷ According to the *Doctrine*, the information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, action or inaction, and human and automated decision-making. See appendix I for additional information about the evolution of information as a joint function and about operations in the information environment.

The economic and social revolutions wrought by the industrial age rapidly changed how wars were fought and won in the 19th and 20th centuries. Leaders who grasped the implications of those changes developed the strategies and designed operations that led to success, while those who did not were doomed to failure.

Today, in the midst of an information age that has similarly transformed economies and societies, we must likewise adapt our thinking and deepen our understanding if we hope to succeed in the 21st-century conflicts.

Within the changing environment, information may prove to be the preeminent commodity and decisive factor in military operations. [emphasis added]

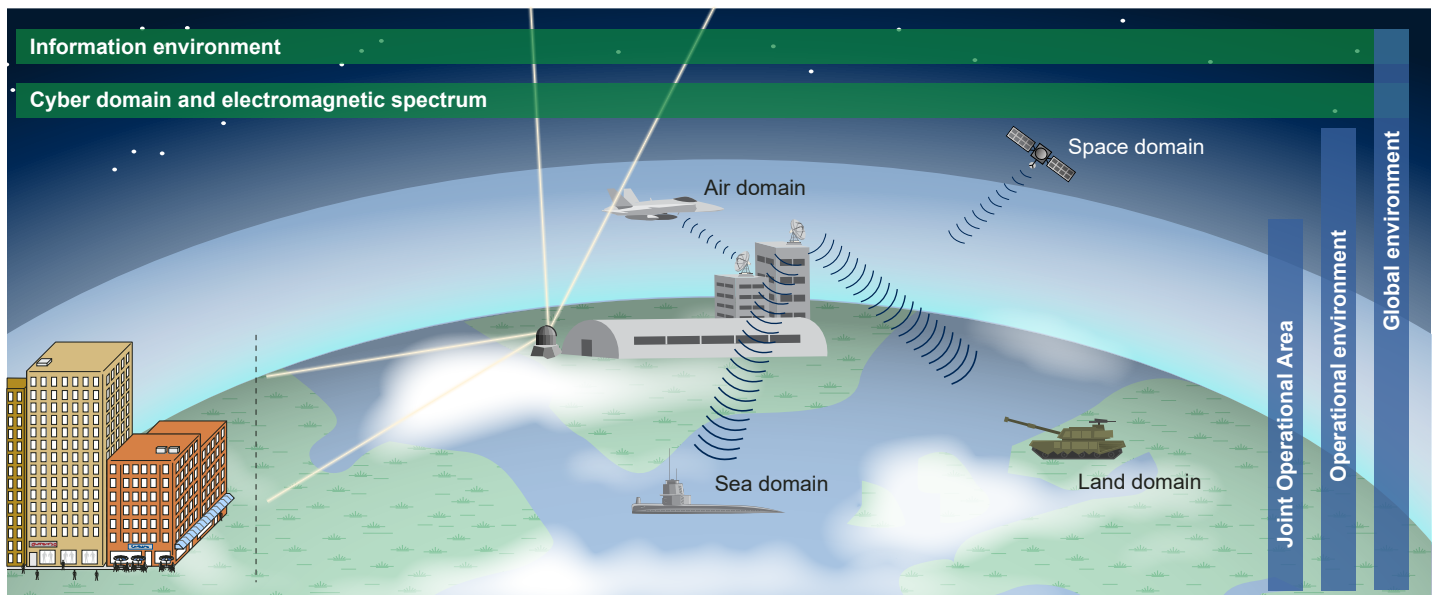
– Brigadier General Alexis Grynkewich, Deputy Director for Global Operations, Joint Staff J7; Joint Force Quarterly 89, 2nd Quarter 2018, “Introducing Information as a Joint Function”

⁵Cognitive security is the field of online and offline influence—and protection from influence—of individuals, groups, organizations, and societies, according to the Applied Research Laboratory for Intelligence and Security (University of Maryland).

⁶Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (July 25, 2018).

⁷Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Mar. 25, 2013, incorporating Change 1, July 12, 2017).

Figure 3: Illustration of Activities in the Operational Environment Relying on the Information Environment



Source: GAO analysis of Department of Defense information. | GAO-22-104714

Since 2019, we have issued a series of reports assessing DOD operations in the information environment—including DOD cyberspace operations, information operations, and EMS operations.⁸ We have also issued reports on emerging threats to national security, threats attributed to emerging technology in the information environment (including 5G wireless technologies and Internet-of-Things devices), cybersecurity, and units that conduct operations in the information environment.⁹ In 2021, we testified that DOD needs to act to ensure superiority for EMS operations and DOD information operations need enhanced leadership and integration of capabilities.¹⁰ See our list of related GAO Reports focused on information environment topics at the end of this report.

GAO initiated this review under the Comptroller General’s authority under section 717 of title 31 of the United States Code in order to inform the Congress on the importance of the information environment, how DOD’s components understand the information environment, the threats and key challenges to the information environment, and DOD’s plans to operate in and protect its interests in the information environment.

This report describes DOD’s use and protection of the information environment through the following six key elements: (1) ubiquitous and malign information; (2) the information environment’s effects on DOD’s mission; (3) threat *actors* to the DOD information environment; (4) threat *actions* to the DOD information environment; (5) institutional challenges DOD faces in using the information environment; and, (6) emerging technologies that can enable or adversely affect DOD’s missions in the information environment. The report also describes DOD actions taken from October 2018 through December 2021 and actions planned through September 2023 to use and protect the information environment.

To assess all of our objectives, we administered a standardized questionnaire to a non-generalizable sample of 25 DOD organizations. These organizations included the Office of the Secretary of Defense; the Joint Staff (to include the Joint Chiefs of Staff and the Joint Information Operations Warfare Center (JIOWC)); five military services; all 11 combatant commands; and the following defense agencies and organizations: Defense Advanced Research Projects Agency (DARPA), Defense Digital Service (DDS), Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA), Defense

⁸GAO, *Cyberspace Operations: DOD Has Authorities and Organizations in Place, but Policies, Processes, and Reporting Could Be Improved*, GAO-20-13C (Washington, D.C.: Sept. 28, 2020); *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019); and GAO, *Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issued to Help Ensure Superiority*, GAO-21-64 (Washington, D.C.: Dec. 10, 2020).

⁹GAO, *National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies*, GAO-19-204SP (Washington, D.C.: Dec. 13, 2018); *National Security: Actions Needed to Address 5G Telecommunications Risks*, GAO-21-256SU (Washington, D.C.: Mar. 5, 2021); *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020); *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241 (Washington, D.C.: Apr. 13, 2020); and *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*, GAO-19-570 (Washington, D.C.: Aug. 15, 2019)

¹⁰GAO, *Electromagnetic Spectrum Operations: DOD Needs to Take Action to Ensure Superiority*, GAO-21-440T (Washington, D.C.: Mar. 19, 2021); and *Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities*, GAO-21-525T (Washington, D.C.: Apr. 30, 2021).

Media Activity (DMA), and the National Security Agency (NSA).¹¹

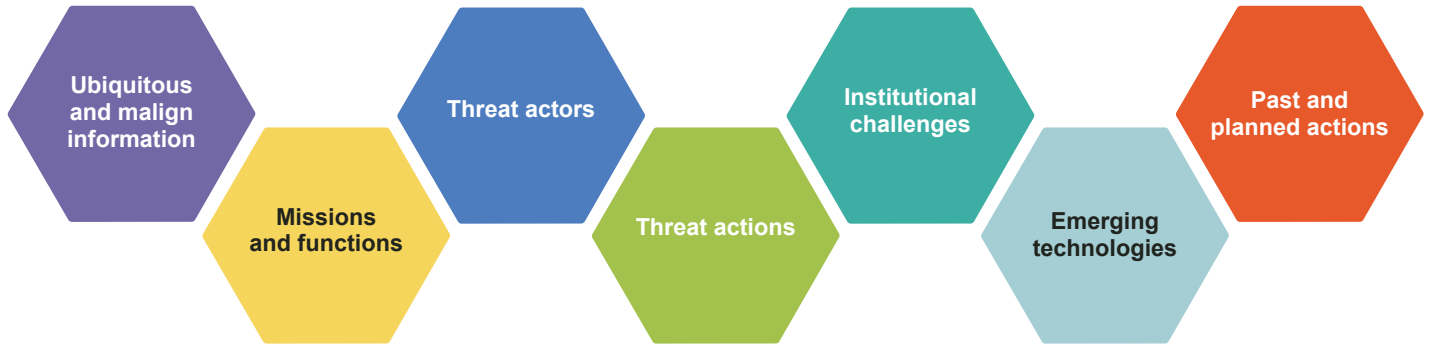
We also administered a second questionnaire to the leadership of each of these 25 DOD organizations asking about the information environment's effect on their organizations. We interviewed officials from nine DOD components to obtain background information about the information environment and to test and refine our questionnaires in addition to subject matter experts external to DOD. We also reviewed 35 documents about strategy, policy, doctrine, and other guidance from DOD and other federal government agencies, as well as 69 white papers, studies, and news articles related to the information environment. See appendix II for a detailed description of our methodology.

We conducted this performance audit from January 2021 to September 2022 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.

¹¹Although the U.S. Coast Guard is a military service, we did not include it in the scope of this engagement because it is a part of the Department of Homeland Security.



Profile Sheets

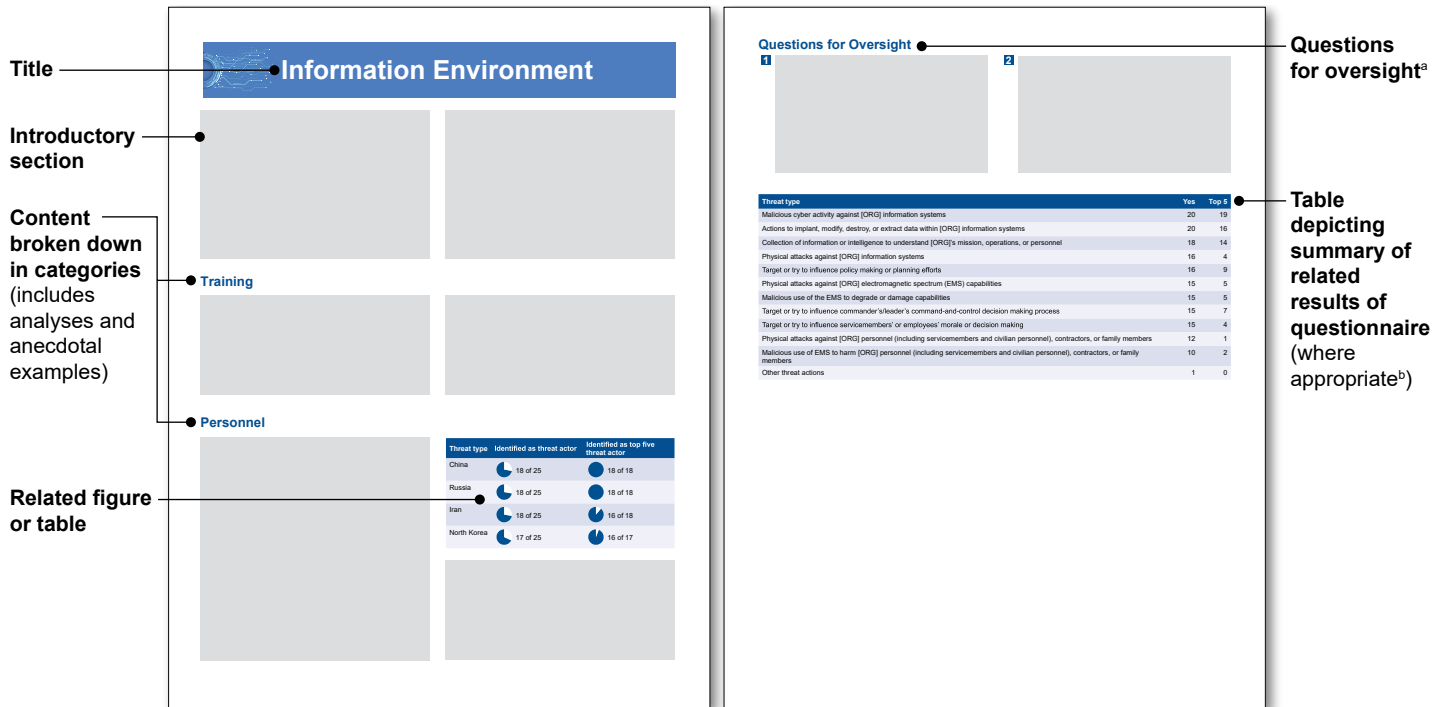


Source: GAO. | GAO-22-104714

This report is composed of profile sheets that describe DOD’s use and protection of the information environment through the following six key elements: (1) ubiquitous and malign information; (2) the information environment’s effect on DOD’s missions and functions; (3) threat *actors* to the DOD information environment; (4) threat *actions* to the DOD information environment; (5) institutional challenges DOD faces in using the information environment; and, (6) emerging technologies that can enable or adversely affect DOD’s missions in the information environment. A seventh profile sheet describes actions DOD has taken over the past 2 fiscal years and plans to take in the near future to use and protect the information environment.

Each profile sheet is composed of similar components, as depicted in figure 4 below.

Figure 4: Profile Sheet Template



Source: GAO. | GAO-22-104714

^aQuestions for Oversight were developed based on our discussions with DOD officials and external subject matter experts, analysis of DOD’s responses to our component and leadership questionnaires, and a review of recent GAO work relevant to the information environment.

^bFive of the seven profile sheets had results from our questionnaire that could be quantitatively analyzed. For these five profile pages, we included a summary table depicting the results of those questions. The other two profile pages were based on qualitative analyses of information gathered from the questionnaire as well as documents the team reviewed.



Ubiquitous and Malign Information

Information is the foundation of all human interaction, as noted in Marine Corps' Information doctrine.¹² It is the basis for how we sense, make sense of, and interact with our environment with each other. The modern escalation in the volume and interconnectedness of data has changed the landscape of information and national security. Within the information environment, individuals, special interest groups, and adversaries can target the cognitive foundations of individuals—beliefs, norms, emotions, experiences, and mental health—using data and information to influence decisions and actions for purposes either benign or malign.

The DOD components we surveyed, subject matter experts we interviewed, and articles and journals we reviewed emphasized that adversaries can leverage data and information to undermine our national security goals. These officials and documents highlighted ubiquitous information, disinformation, misinformation, and malinformation as mechanisms for undermining those goals.

Ubiquitous Information

Data are ubiquitous. Modern devices, systems, and locations generate, retain, and share enormous volumes of data for broader use. This includes information collected from service members', employees', contractors', and family members' personal devices, online accounts, credit reports, online searches, and online purchases. As noted in the *DOD Data Strategy*, this could also include information collected from DOD weapons platforms, connected devices, sensors, training facilities, test ranges, and business systems.¹³ These data can be collected and shared publicly or can be acquired from data brokers. For example, as shown in figure 5, certain activities that could indicate a potential deployment of a military unit can be gathered from publicly available information, data brokers, and/or accessing contractors' networks.

DOD faces a number of risks stemming from the advance of technological capabilities (such as 5G wireless, artificial intelligence (AI), and other data-based technologies) and the continued aggregation and analysis of data on individuals' personal and professional lives. Those risks include force protection, operations security, safety and security of

Figure 5: Ubiquitous Public Information Can Foreshadow a Military Deployment



-  Social media, traffic applications, and other phone tracking with proximity notifications
-  Hometown school announces plan to create patriotic signs to show their support for departing soldiers
-  Commercial satellite imagery
-  Social media activity and sudden inactivity
-  Hometown news covers reserve transport units activating
-  Contract awarded for logistics services in deployed locations announced
-  Local paper announces arrival of unit for Mission Readiness Exercise
-  Global media depicts U.S. and partner forces building up
-  Local foreign citizens observe activity and spread information; social media traffic trends high

Source: GAO analysis of University of Maryland's Applied Research Laboratory for Intelligence and Security information; U.S. Army/1st Lt. H. Chan (photo). | GAO-22-104714

family members, remote surveillance (also known as ubiquitous technical surveillance), and intelligence collection. For example, an academic paper about special operations in a 5G environment highlighted the pending challenges of special operations units' ability to conceal their identities and operations in a 5G environment where information will be integrated

¹²U.S. Marine Corps, *Information*, Marine Corps Doctrinal Publication 8, (June 21, 2022).

¹³DOD, *DOD Data Strategy*, (Sept. 30, 2020).

at unprecedented speeds.¹⁴ See later discussion in our “Emerging Technologies Associated with the Information Environment” profile sheet for additional information about opportunities and threats associated with these and other technologies.

The fusion of ubiquitous information and technology enables individuals, organizations, and nation-states to exploit DOD personnel and their family members with personalized or “micro-targeted” disinformation with the intent of influencing them to act in a manner favorable to the originator’s objectives. As a hypothetical example, micro-targeting could enable foreign intelligence entities to identify DOD personnel who may be more susceptible to (un)wittingly sharing sensitive and classified information. Additionally, one of the subject-matter experts we met with said targets are susceptible to disinformation that fits their beliefs, attitudes, and worldviews. This can lead targets to increase their reliance on disinformation and in some instances make them resistant to attempts to “correct” their views causing them to more strongly accept disinformation. Additionally, according to this expert, biases such as confirmation bias, anchoring bias, and status quo bias can also be exploited through micro-targeting.

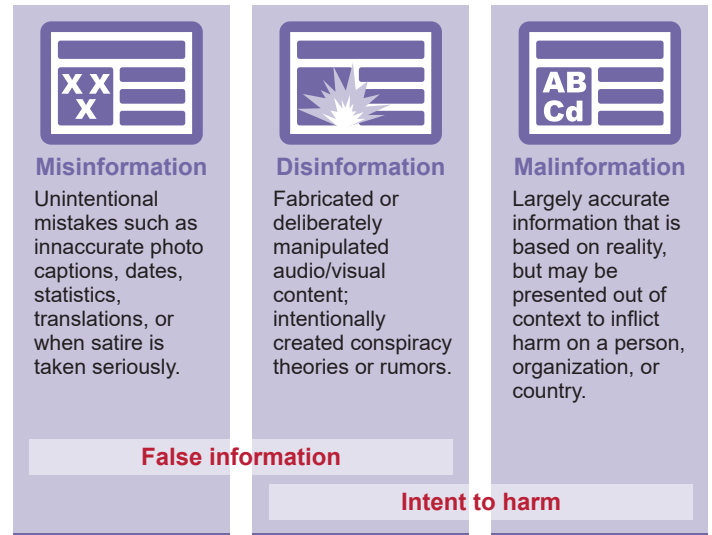
The information environment has become more complicated, more extensive, more ubiquitous, and more important to the outcomes of military operations than ever before.

– “Lessons from Others for Future U.S. Army Operations in and Through the Information Environment,” RAND Corporation

Malign Information (Misinformation, Disinformation, and Malinformation)

DOD guidance states that the effect of information on a recipient is influenced by several factors including 1) whether the information is true, false, or a combination of both; 2) whether the recipients are active (intended) or passive (unintended); and 3) the intent of the source or author of the information. As a result, sources and recipients may have different perspectives on whether information is true, false, or a combination of both. This discrepancy can enable a source or author to use information in a malign way to achieve a specific outcome. We refer to this as malign information. Such information is particularly effective if the recipient perceives the information to be accurate and timely. Malign information typically falls into one of three categories, as illustrated in Figure 6.

Figure 6: Relationship between Misinformation, Disinformation, and Malinformation



Source: GAO analysis of Department of Homeland Security information. | GAO-22-104714

Misinformation. Misinformation is the unintentional spread of inaccurate information. It may occur due to so-called “fog of war” situations in which the accuracy and completeness of information (including videos, emails, messages, photos, and audio communications) may be unavailable. As noted by the Congressional Research Service, another example could be internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. Misinformation can have the effect of sowing divisiveness and chaos in a target society, as the truth becomes harder to discern. Misinformation also poses a significant challenge for DOD’s operations. According to DISA, the shift to a geographically separated workforce has potentially created environments where employees feel disconnected and are more vulnerable to misinformation. For example, in responding to our questionnaire, the Navy said that misinformation about COVID-19 resulted in confusion about the safety of vaccination, which potentially led to reduced readiness.

Disinformation. Disinformation is the deliberate dissemination of false information with the intent to deceive. It poses a critical threat to DOD’s ability to conduct operations and successfully execute its missions and the department remains vulnerable to enemies that seek to use this tool. In 2020, the RAND Corporation characterized the detection of malign information efforts as a critical vulnerability during the War on Terror.¹⁵ RAND pointed out that DOD observed violent extremist organizations

¹⁴M. P. Jones, E. L. McCaslin, *Special Operations in a 5G World: Can We Still Hide In The Shadows?* (Monterey, CA: Naval Postgraduate School, June 2020). For additional information on the implications of 5G wireless technologies, see GAO, *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: Nov. 24, 2020).

¹⁵RAND, *Detecting Malign or Subversive Information Efforts over Social Media Scalable Analytics for Early Warning*, RR4192 (Santa Monica, CA: 2020).

undertaking information campaigns and it did not possess the capability to counter these campaigns.

During combat operations in Iraq and Afghanistan, DOD forces observed that our adversaries leveraged disinformation to influence sympathizers and undermine our presence and actions. For example, according to the Army, during Operation Valhalla in March 2006, a combined battalion of U.S. and Iraqi Special Forces engaged in a firefight with a Jaish al-Mahdi death squad at one of its compounds.¹⁶ During the engagement, the U.S. and Iraqi soldiers destroyed a weapons cache and rescued a badly beaten hostage. However, by the time the soldiers had returned to their base—less than an hour later—someone had returned to the scene, removed the weapons from the bodies of the death squad members, and rearranged the bodies to make it look as if they had been murdered while in the middle of prayer. They then took pictures, uploaded them into the web, and issued a press release explaining that U.S. soldiers had entered a mosque and killed men peacefully at prayer. As a result of this disinformation activity, this special operations unit was not allowed to conduct any military operations for 30 days while the Army conducted an internal investigation.

Malinformation. Malinformation is largely accurate information, but used out of context to mislead, harm, or manipulate. For illustrative purposes, as documented in a congressional hearing and U.S. Marine Corps documents, a scandal broke out in 2017 on a private social media group used by more than 30,000 people—including active-duty Marines and veterans—whereby armed forces members were accused of being involved in the distribution or viewing of private, intimate, or explicit imagery of service members and veterans that were posted without consent from the individuals in those photos. Changing the context of this information—by publicly sharing private imagery—has the potential to undermine unit morale, confidence in leadership, commitment to military values, and safety of victims. For example, as a result of the 2017 scandal, several victims (which included current and former service members) told the press that they were harassed and afraid to leave their house.

Following that scandal, the military identified and took action on other cases where service members were posting non-consensual photos. For example, in response to the revelations, service leadership established task forces to examine the matter and to identify and implement long-term solutions; issued new guidance regarding the use of social media; and required mandatory counseling to assure that service members understood the newly issued guidance. In addition, Congress amended the Uniform Code of

The United States may never again have a “9/11 experience,” whereby Americans agree on the facts, interpretation, and corresponding response in the wake of a major catastrophe. After 9/11, 99.9% of Americans understood and shared the same basic set of facts—the U.S. had been attacked, it had resulted in nearly 3,000 deaths, and that they were perpetrated by Al Qaeda. As we have seen in everything from attacks on our elections to the pandemic, a similar catastrophe today would not elicit the same universal agreement because of how contested the information environment has become.

— GAO interview with Dr. Peter W. Singer, author of *LikeWar: The Weaponization of Social Media* and Senior Fellow at New America

Military Justice to penalize the wrongful distribution of intimate visual images. Ultimately, according to media reports, multiple service members were convicted and discharged.

Questions for Oversight

- 1 What action is the department taking to inform service members and their families about, and protect them from misinformation and disinformation?
- 2 What steps have each of the components taken to clearly communicate that malinformation generated by service members, civilian employees, and contractors is unacceptable and that they will be held accountable should they disseminate such material?
- 3 What can DOD do to educate DOD personnel (including military, civilians, contractors, and dependents) to better protect themselves from threat actors who can micro-target them as a result of publicly available information?
- 4 What action is DOD taking to manage the publicly available information of its personnel, units, and operations?

¹⁶U.S. Army Combined Arms Center, *Military Review: The Professional Journal of the U.S. Army* (Fort Leavenworth, KS: January-February 2009).



Missions and Functions Affected by Operations in the Information Environment

According to the 2022 National Defense Strategy, DOD will contribute to advancing and safeguarding vital U.S. national interests—protecting the American people, expanding America’s prosperity, and realizing and defending our democratic values.¹⁷ To successfully meet this enduring mission, DOD’s components rely on technology, the EMS, and transmitted data to analyze and act on information. The degree to which each mission or function is affected by the information environment varies.

We asked 25 DOD components to select from a list of 17 missions and functions (with an opportunity to write in others) that are affected by the information environment. We also asked the components to then identify the five missions and functions that they consider to be most affected by the information environment.¹⁸ In their responses, DOD components consistently identified communications; security; development of policy, plans, or doctrine; coordination with allies and partners; the conduct of military operations; and command-and-control decision-making.

Below are anecdotal examples provided by the DOD components in their component questionnaires that illustrate their perspectives on the categories of missions and functions most affected by the information environment.

Communications

Overall, all 25 components identified “communications” as being affected by the information environment and 16 components identified communications as being among the five most affected by the information environment, as illustrated by the following examples from their questionnaire responses.

- The Army noted that communications and communications systems and capabilities move in and through the information environment. Video teleconferencing, voice over internet protocol, classified and unclassified email, and telephone systems are all operating in the information dimension. These communications capabilities allow for the synchronization of global efforts.
- U.S. Southern Command (SOUTHCOM) stated that all of its operations, activities, and

investments follow a strategic communications plan that encompasses the use of information-related capabilities. SOUTHCOM added that it ensures that these information-related capabilities support broader national defense and foreign policy objectives through the use of various strategic communications working groups, information operations synchronization meetings, and routine engagements with interagency partners.

- U.S. Strategic Command (STRATCOM) stated that the use of the information environment ensures the ability to transmit threat and force information to STRATCOM and national leadership as well as disseminating clear force directions to combat forces.

Security

Overall, all 25 components identified security (e.g., operations security and information security) as being affected by the information environment and 11 components identified security as being among the five most affected by the information environment, as illustrated by the following examples.

- The Air Force and U.S. Transportation Command (TRANSCOM) indicated that the aggregation of publicly available information, in the form of social media posts or separate activities in the supply chain can provide adversaries with insight into current and future operations. TRANSCOM added that the protection of critical information spanning the command’s operations and military activities is a continuous effort.
- One subject matter expert with whom we spoke noted the potential risk to military operations from publicly available information. He explained how even mundane items like contracts awards or local school farewell events for deploying units can provide intelligence for adversaries. A second expert concurred, commenting DOD is “hemorrhaging data” because it is unable to prevent the extraction and theft of data and protect the personally identifiable information of its service members.

¹⁷DOD, Fact Sheet: 2022 *National Defense Strategy* (March 2022).

¹⁸In our questionnaire, DOD components had the ability to identify those missions/functions as being one of the five missions/functions that they consider to be “most impacted” by the information environment. We let each of the 25 DOD components to whom we sent our questionnaire to use its own reasoning and understanding to guide responses and interpretation of what constituted something as “most impacted.” For this report, we conform to GAO’s style and use the word “affected” when reporting on questionnaire responses about DOD being “impacted” by the information environment.

- The Air Force stated in its questionnaire response that the service has launched a Digital Literacy competency program that would apply to its personnel at all service ranks, grades, and career fields. As previously described in this report, ubiquitous information presents a number of national security risks.

Policy, Plans, or Doctrine Development

Overall 22 of the 25 components identified “policy, plans, or doctrine development” as being affected by the information environment. Twelve components identified policy, plans, or doctrine development as being among the five most affected by the information environment, as illustrated by the following examples from their questionnaire responses.

- U.S. Northern Command (NORTHCOM) stated that its success depends on thorough analysis and understanding of the operational environment and information environment. NORTHCOM also stated that understanding the information environment—the kind of information, how it is generated, where it resides, how it interrelates, how it is consumed, how it may be exploited, etc.—is the key to achieving objectives or desired end states in support of any successful policy, plan, or doctrine.
- The JIOWC stated that the elevation of information as a joint function in 2017, the 2018 *Joint Concept for Operating in the Information Environment*, and the forthcoming issuance of Joint Publication 3-04 shows DOD understands the importance of the information environment to operations. The JIOWC noted that the *Joint Concept* describes the problem set and the forthcoming Joint Publication 3-04 will explain how to operationalize and conduct military operations and ensure information is part of operational art. It added that without guidance on how to operate in the information environment, the U.S. cedes the information environment to adversaries. However, an official from the Office of the Under Secretary of Defense for Policy told us that while Joint Publication 3-04 will establish a new, joint lexicon for information environment-related terms and definitions, service-level doctrine may not necessarily align with it. Therefore, the military services would need to update their doctrine documents for all of DOD to have a consistent lexicon.

Coordination with Allies and Partners

Overall 22 DOD components identified “coordination with allies and partners” as being affected by the

information environment with 10 identifying it as being among the five most affected. Components cited it as being core to completing their missions and to protecting national security. In responding to the questionnaire, U.S. Indo-Pacific Command (INDOPACOM) reported that local foreign military officials are less inclined to speak negatively about strategic competitors or confront malign influence in the same manner as the United States. The command added that this is particularly the case when in matters such as maritime presence and freedom of navigation operations in the South China Sea.

- The 2022 National Defense Strategy fact sheet recognizes the value of coordinating with allies and partners that are mutually beneficial alliances. These partnerships are critical to achieving our objectives, as demonstrated by the unified response to Russia’s further invasion of Ukraine.¹⁹ According to a 2019 RAND study, steps to enhance coordination could include supporting and engaging multilateral fusion centers on gray-zone matters as well as regional multilateral crisis avoidance and consultation organizations.²⁰

All activity in the information environment impacts broader military operations, activities and investments. Leading with information entails designing component campaigns and operations directly around shaping perceptions and behaviors of relevant actors and target audiences of interest. [...] The operational environment is comprised of the information environment and physical environment. All future strategy and planning should clearly articulate the role of the information environment and information related capabilities in achieving desired end states and objectives. Air Force actions in the information environment require an integrated strategic plan and are part of larger Whole-of-Government approach.

— Lt. Gen. Mary O’Brien, Maj. Gen. Charles Corcoran, Lt. Gen. Clinton Hinote; U.S. Air Force response to GAO leadership questionnaire

Conduct Military Operations

Overall, 21 of the 25 components identified “conduct military operations” as being affected by the information environment and 18 components identified conduct of military operations as being among the five most affected by the information environment, as illustrated by the following examples.

- In 2020, we reported that DOD operations in all domains—air, land, sea, space, and cyber—depend on the ability to use and control the EMS.²¹ However, technological advances could result in EMS-dependent capabilities being among the first to be targeted in a conflict. According to DOD, adversaries have perceived that the department’s reliance on the EMS makes its operations vulnerable. Similarly, we and a congressional Future of Defense Task Force

¹⁹DOD Fact Sheet: 2022 *National Defense Strategy*.

²⁰RAND, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War* (2019).

²¹GAO-21-64.

have reported that the EMS-dependent GPS could be a single point of failure for the United States military.²² These vulnerabilities leave DOD's ability to accurately navigate in a contested environment in danger.

- The U.S. Space Force (Space Force) stated it relies upon the information environment to gather, store, analyze, fuse, exploit, and assess data when making decisions and taking actions in the space domain. In Space Force's capstone publication, *Spacepower: Doctrine for Space Forces*, the service noted that because of the prevalence of remote operations, the EMS is the primary conduit through which the control and exploitation of the space domain is achieved.²³
- The Navy stated that its maritime operations, including freedom of navigation operations around the world and coalition operations, benefit from the information environment. Navy officials stated that the information environment is a force multiplier for their objectives.

Command-and-Control Decision-Making

Overall, 21 of the 25 components identified "command-and-control decision-making" as being affected by the information environment and 15 components identified command-and-control decision-making as being among the five most affected by the information environment, as illustrated by the following examples from their questionnaire responses.

- STRATCOM stated that the information environment influences the command leadership decision-making process. Similarly, NORTHCOM noted that information dominance and decision superiority relies upon timely and accurate information from a variety of reliable and authoritative sources.
- U.S. Africa Command (AFRICOM) stated that the information environment is critical to the development of request for forces, requests for support, requests for information, and issuing orders. These actions allow AFRICOM's headquarters to delegate tasks, command operational forces on the African continent, and give specific directions and instructions for the scope of operations.
- The Marine Corps similarly acknowledged that command-and-control decision-making is a key element within the information environment. It identified the service's establishment of an

Information Command Center as a testament to this critical aspect.

Questions for Oversight

- 1 How can DOD improve digital literacy for service members to understand the importance information plays in protecting the United States?
- 2 How can DOD develop consistent policies, plans, doctrine, and a common lexicon for both its components and the Department as a whole?
- 3 What actions can DOD take to ensure that command-and-control decisions are made with timely, accurate, and reliable information?

²²GAO, *Technology Assessment: Defense Navigation Capabilities*, GAO-21-320SP (Washington, D.C.: May 10, 2021); and House of Representatives Armed Services Committee, *Future of Defense Task Force Report* (Sept. 23, 2020).

²³Department of Defense, United States Space Force, *Spacepower: Doctrine for Space Forces* (June 2020).

Table 1 shows how DOD components identified missions and functions that are affected by the information environment in their responses to our questionnaire.

Table 1: DOD Component Responses to Missions and Functions Affected by the Information Environment

| Missions and functions | Yes | No | Unknown | Not applicable | Top five most affected |
|---|-----|----|---------|----------------|------------------------|
| Communications | 25 | 0 | 0 | 0 | 16 |
| Security (e.g., operations security and information security) | 25 | 0 | 0 | 0 | 11 |
| Business operations | 23 | 1 | 1 | 0 | 5 |
| Policy, plans, or doctrine development | 22 | 2 | 0 | 1 | 12 |
| Coordination with allies and partners | 22 | 0 | 1 | 2 | 10 |
| Intelligence and counterintelligence activities | 22 | 0 | 0 | 3 | 9 |
| Day-to-day decision-making | 22 | 3 | 0 | 0 | 4 |
| Maintain organization cohesion, morale, or discipline | 22 | 2 | 1 | 0 | 0 |
| Conduct military operations | 21 | 0 | 0 | 4 | 18 |
| Command-and-control decision-making | 21 | 2 | 0 | 2 | 15 |
| DOD coordination with other agencies | 21 | 2 | 1 | 1 | 3 |
| Research and Development | 21 | 1 | 1 | 2 | 3 |
| Acquire and sustain equipment | 21 | 3 | 1 | 0 | 2 |
| Hire, train, or retain personnel | 20 | 3 | 2 | 0 | 3 |
| Provide logistical support | 18 | 1 | 2 | 4 | 1 |
| Oversight of lower echelon organizations | 17 | 3 | 1 | 4 | 1 |
| Conduct law enforcement activities | 11 | 1 | 4 | 8 | 1 |
| Other missions/functions | 7 | 0 | 0 | 0 | 0 |

Source: GAO analysis of Department of Defense (DOD) components' responses to GAO's questionnaires. | GAO-22-104714

Note: The "Top Five" column shows that a component selected the mission/function as being one of the five missions/functions that they consider to be "most impacted" by the information environment. We let each of the 25 DOD components to whom we sent our questionnaire to use its own reasoning and understanding to guide responses and interpretation of what constituted something as "most impacted." For this report, we conform to GAO's style and use the word "affected" when reporting on questionnaire responses about DOD being "impacted" by the information environment.



Threat Actors Associated with the Information Environment

As articulated in the 2021 *Interim National Security Strategic Guidance*, the distribution of power across the world is changing, creating new threats. China has rapidly become more assertive; Russia remains determined to enhance its global influence and play a disruptive role on the world stage; Iran and North Korea continue to pursue game-changing capabilities and technologies, while threatening U.S. allies and partners and challenging regional stability; and violent extremism, both domestic and international, remain significant threats.²⁴ Similarly, the Office of the Director of National Intelligence's 2022 *Annual Threat Assessment* identified these nation-states and non-state actors (such as terrorists and transnational criminal organizations) as top threats to global security.²⁵

We asked 25 DOD components to select the actors that pose a threat to their organization in the information environment, and identify the five threat actors they consider to be most important.²⁶ In our questionnaire, we provided DOD components with 12 nation-state and non-state response options and an opportunity to write in others. What follows are anecdotal examples provided by the DOD components in their questionnaires that illustrate their perspectives on nation-state and non-state actors that they consider to pose a threat in the information environment.

Nation-State Threat Actors

In our questionnaire, we listed the four nation-state actors identified in the *Interim National Security Strategic Guidance*—China, Russia, Iran, and North Korea. Components also had the ability to identify others, though only one component identified another nation-state in its response.



According to DOD, China's leaders view achieving "information dominance" and denying adversaries the use of the EMS as being necessary to seize and maintain the strategic initiative in a conflict.²⁷ As part of its efforts to restructure the People's Liberation Army for modern warfare, China's military's

highest decision-making body established the Strategic Support Force in 2015. This force is to centralize the People's Liberation Army's strategic space, cyber, electronic, and psychological warfare missions and capabilities. Twenty-two of the 25 DOD components we contacted identified China as posing a threat in the information environment, as illustrated by the following examples.

- The Air Force stated that China conducts a number of operations in the information environment that threaten Air Force missions and operations. For example, China maintains a worldwide information collection program to advance its weapons development programs and national influence/disinformation activities. The Air Force added that the People's Liberation Army has targeted critical Air Force information by conducting sophisticated computer network intrusion and data exfiltration operations against the Air Force and its industry partners.²⁸
- The Space Force and SPACECOM stated that China is developing a broad range of counter-space weapons to deny, degrade, and destroy U.S. space assets. These weapons include attributable and non-attributable kinetic and non-kinetic systems able to achieve reversible and irreversible effects making them potentially effective at all levels of competition and conflict. As noted in the United States Space Priorities Framework, space underpins our national security and ability to respond decisively to crises around the world. Information collected from space informs national decision makers about evolving threats to U.S., allied, and partner interests.
- AFRICOM identified China as a threat and noted that its infrastructure programs on the African continent are likely to enhance its ability to exert influence in the information environment.²⁹ China's effort to build a naval base on the Atlantic coast of Africa poses a threat in that it represents

²⁴White House. *Interim National Security Strategic Guidance* (Washington, D.C.: March 2021).

²⁵Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: March 8, 2022).

²⁶We used the term "most important" in the questionnaire sent to all 25 DOD components. We let each DOD component use their own reasoning and understanding to guide their responses and interpretation of what constituted something as "most important."

²⁷DOD, *Military and Security Developments Involving the People's Republic of China: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2000*, (2021).

²⁸According to the Air Force, China has targeted sensitive data and technology, trade secrets, intellectual property, and personally identifiable information from sectors of the economy that the Air Force relies on including managed service providers, semiconductor companies, defense industries, unsecured communication systems, social media, public forums and scientific/academic institutions.

²⁹According to DOD, China's activities are often undertaken as a part of its Belt and Road Initiative and Digital Silk Road.

a sizeable economic endeavor, with infrastructure, agreements, and contracts. China can leverage these investments to influence partner behaviors and regional perceptions and public opinion; likely to the detriment of the United States.

"Russia and China, as well as non-state actors understand that they have real-time access to a global audience. With first-mover advantage and by flooding the information environment with deliberately manipulated information, these actors can gain leverage to threaten our interests... Our Soldiers, Sailors, Marines, Airmen, Guardians, civilians, and their families are part of the American public directly targeted by malign actors' disinformation, misinformation, and propaganda. DOD views this as a critical force protection issue."

— Christopher Maier, Assistant Secretary of Defense, Special Operations and Low-Intensity Conflict, testimony before the House Armed Services Committee, Subcommittee on Intelligence and Special Operations, March 16, 2021

missions, intentions, and motivations to increase negative perceptions of DOD among foreign audiences.

A recent RAND Corporation study reported that a number of steps can improve the U.S.' ability to counter information campaigns. These include exposing Russian propaganda, building the resilience of populations most susceptible to Russian propaganda, promoting local media that counter propaganda, and tracking and analyzing the content of Russian media to maintain a high awareness of the threat.³²

Iran and North Korea

Russia

Russia's use of tactics below the threshold of war is well documented and persistent. According to RAND, these actions take place in a variety of domains, from cyber and economics to information and politics. They are aimed toward various objectives, such as sowing dissent among national and local communities, steering them toward a more pro-Russia stance, or intimidating them.³⁰ Twenty-two of the 25 DOD components we contacted also identified Russia as posing a threat in the information environment, as illustrated by the following examples.

Overall, at least 18 of the 25 DOD components included Iran or North Korea in their identification of most important threats, but few provided examples of how or why those countries are threats in the information environment.

- NORTHCOM stated that Russia sponsors malign cyber activity against a U.S. oil pipeline, disrupting the flow of oil within the United States, instilling doubt in America's ability to defend itself against cyber threats, and heightening inflation in the U.S. economy.
 - The intelligence community attributed the SolarWinds Orion software breach in 2020 to the Russian foreign intelligence service.³¹ This cyberattack exploited a software vulnerability that provided access to U.S. government and private sector computer systems to Russian intelligence. The attack compromised the networks of multiple U.S. government agencies and provided the opportunity for espionage. Since then, the U.S. government has made cybersecurity and policy changes to address these threats.
 - SOUTHCOM stated that Russian media regularly skews, twists, and misrepresents information to Latin American audiences on DOD activities,
- The majority of DOD components responding to the questionnaire (22 of 25) identified Iran as a threat within the information environment. The Office of the Director of National Intelligence's 2022 *Annual Threat Assessment* states, "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data." In February 2022, multiple government organizations released a joint Cybersecurity Alert highlighting a group of Iranian government-sponsored advanced persistent threat actors conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors in Asia, Africa, Europe, and North America.³³
 - Eighteen DOD components—including INDOPACOM, DISA, and NORTHCOM—identified North Korea as a top five most important threat actor. The components attributed to it similar threat actions committed by Chinese and Russian state actors to degrade DOD systems and operations, and to contribute to mis- and disinformation campaigns against U.S. service members.

³⁰RAND Corporation, *U.S. Strategic Competition with Russia; A RAND Research Primer* (Santa Monica, CA: RAND Corporation, 2022).

³¹GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 (Washington, D.C.: Jan. 13, 2022).

³²RAND Corporation, *U.S. Strategic Competition with Russia; a RAND Research Primer* (Santa Monica, CA: RAND Corporation, 2022).

³³Cybersecurity & Infrastructure Security Agency (CISA), "Iranian Government-Sponsored Actors Conduct Cyber Operations against Global Government and Commercial Networks," Alert AA22-055A (Feb. 24, 2022), accessed May 27, 2022, <https://www.cisa.gov/uscert/ncas/alerts/aa22-055a>. Organizations that were involved in developing the joint advisory include the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, U.S. Cyber Command, and the United Kingdom's National Cyber Security Centre.

Non-State Threat Actors

In our questionnaire, we also asked specifically about a variety of non-state threat actors and encouraged components to write in others. In response to our questionnaire, DOD components highlighted threats associated with insider threats, foreign terrorists, lone-wolf actors, transnational criminal organizations, and corporations.³⁴

Insider Threats. DOD components identified insider threats—including intentional or unintentional actions—as a significant challenge. The Office of the Secretary of Defense and the Defense Media Activity both identified insider threats as risks to operational and information security. The Space Force stated that a single disgruntled individual with access to sensitive or classified information can easily cause significant damage to U.S. organizations by stealing and then releasing this information to foreign governments or the media.

Foreign Terrorists. DOD components identified foreign terrorists (such as ISIS, Al-Shabaab, Boko Haram, etc.) as threat actors in the information environment. AFRICOM identified violent extremist organizations as threats to operations in its area of responsibility, while INDOPACOM stated that violent extremist organizations are using the narrative of the Taliban’s victory over the U.S. in Afghanistan to influence extremists in the Philippines and Indo-Pacific region. NORTHCOM also stated that foreign terrorist operatives target sympathetic U.S. service members on social media, attempting to convince them to commit an active-shooter scenario at a U.S. military installation to atone for perceived atrocities committed by the U.S.

Transnational Criminal Organizations. DOD components, including NORTHCOM and the Marine Corps, identified transnational criminal organizations as threat actors in the information environment. For example, the Marine Corps noted that transnational criminal organizations (among other threat actors) seeking financial gains target Marines via social media.

“Lone-Wolf” Individuals. DOD components identified “lone-wolf” individuals as being threats generated by actions in the information environment. For example, officials from the Air Force stated in its questionnaire responses that adversary and violent extremist social media influence campaigns can inspire individual lone-wolf actors to take action against Air Force presence worldwide. In other

instances, the social media influence campaigns can focus on individual Air Force personnel, which could degrade overall morale, unit cohesion, and confidence in leadership.

U.S. or Foreign Corporations. In addition to these threat actors, DOD components also identified U.S. or foreign corporations. The Defense Media Activity stated that when U.S. or foreign corporations use or sell freely posted DOD videos or images out of context (i.e., malinformation) for their profit-oriented goals or to present a message inaccurately (i.e., misinformation or disinformation), it can undermine the public’s confidence in DOD media. A subject matter expert told us that corporations could also be a threat to the information environment. According to the expert, corporations acting with quasi-sovereign status, in combination with their information and influence capabilities, can make them formidable challenges to operating in the information environment. We reported in 2018 that non-state actors, such as private corporations, could emerge as a threat as these organizations may obtain resources that could grant them more influence than the state.³⁵

Questions for Oversight

- 1 Should DOD organize the Office of the Secretary of Defense and other DOD components to have centralized or distributed information-based organizations focused on its space, cyber, electronic, and information warfare missions and capabilities?
- 2 How do DOD policies and approaches to addressing threats in the information environment posed by nation-state actors differ from those designed to address non-state actors?
- 3 What actions can DOD take to better protect itself from insider threats? What actions can preemptively address situations that may lead a service member or other DOD employee to act against the interests of DOD?
- 4 What actions can DOD take to form better relationships with U.S. and foreign corporations to improve cooperation and fight adversary information and influence campaigns?

³⁴The Office of the Director of National Intelligence defines an insider threat as the threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. In the questionnaire that we transmitted to DOD components, we referred to “transnational organized criminal organizations;” however, the Office of the Director of the National Intelligence uses the term “transnational criminal organizations.” Consequently, for the purpose of this report, we will consistently refer to this threat actor consistent with the Office of the Director of the National Intelligence.

³⁵GAO-19-204SP.

Table 2 shows how DOD components identified actors that pose a threat to their organization in the information environment in their responses to our questionnaire.

Table 2: DOD Component Responses to Information Environment Threats

| Threat actor | Yes | No | Unknown | Top five most impacted |
|---|-----|----|---------|------------------------|
| China | 22 | 0 | 2 | 22 |
| Russia | 22 | 0 | 2 | 22 |
| Iran | 22 | 0 | 2 | 20 |
| North Korea | 21 | 1 | 2 | 18 |
| Insider threats (intentional and/or unintentional) | 21 | 0 | 3 | 6 |
| Foreign terrorists (e.g., ISIS, Al-Shabaab, Boko Haram, etc.) | 20 | 0 | 4 | 14 |
| Transnational organized criminal organizations | 17 | 4 | 3 | 5 |
| Individuals/lone-wolf actors (excluding insider threat) | 16 | 2 | 6 | 1 |
| U.S. domestic violent extremists | 13 | 5 | 6 | 0 |
| U.S. or foreign corporations | 11 | 8 | 5 | 1 |
| Other threat actors | 7 | 0 | 0 | 1 |
| Special interest groups | 4 | 7 | 13 | 0 |
| Allies or partners | 3 | 15 | 6 | 0 |

Source: GAO analysis of Department of Defense (DOD) components' responses to GAO's questionnaires. | GAO-22-104714

Note: In our questionnaire, we asked DOD components to identify actors that pose a threat to their organization in the information environment, and which five of those identified actors that they consider to be most important. The "Top Five Most Important" column notes that a component selected a specific threat actor as one of the five threat actors that they consider to be most important. We used the term "most important" in the questionnaire sent to all 25 DOD components. We let each DOD component use its own reasoning and understanding to guide responses and interpretation of what constituted something as "most important."



Threat Actions Associated with the Information Environment

Threat actors operate in a number of ways within the information environment that adversely affects DOD personnel and capabilities. Those actions include malicious cyber activities that modify, delete, or extract data; the use of the EMS to disrupt or influence DOD information systems and operations; intelligence collection against DOD; EMS attacks on DOD personnel; physical attacks on systems; and influence campaigns to affect decisions made by commanders and leaders, as depicted in figure 7.

We asked 25 DOD components to select actions that they consider to be a threat to their organization in the information environment. In our questionnaire, we provided DOD components with 11 response options and an opportunity to write in others. In responding to the questionnaire, each of the 11 response options was chosen at least once by more than 50 percent of DOD components and every option was identified as most important at least once; thus, showing the diversity of actions that threat actors could leverage in this battlespace.

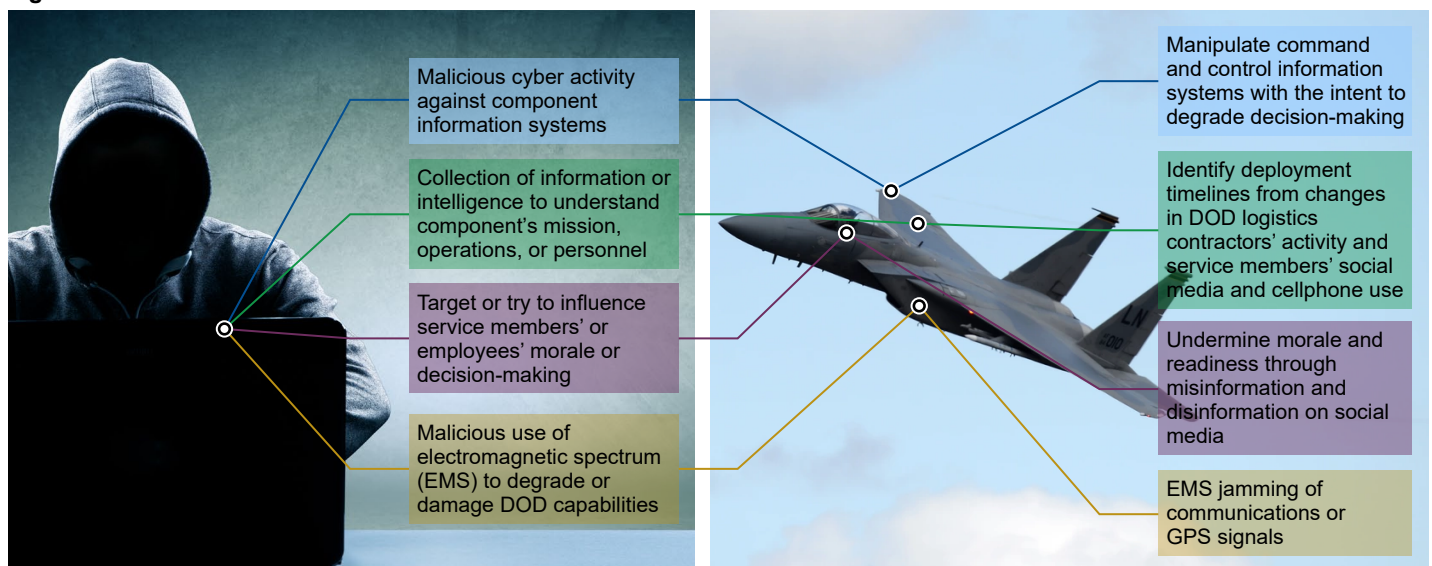
Below we have highlighted anecdotal examples of cyberspace threats, information or intelligence collection threats, influence threats, and electromagnetic spectrum threats, based on information from the DOD component questionnaires, our literature review, and our prior work.

Cyberspace Threats

In our questionnaire, we asked specifically about a variety of cyber threats to information systems. In response to our questionnaire, 24 of 25 components identified two cyber-related threat actions—“malicious cyber activity against component information systems” and “actions to implant, modify, destroy, or extract data within component information systems.” Components provided multiple examples of those threats, including the following:

- The Marine Corps stated that threat actors regularly use malicious code to probe and attack the boundaries of its information systems. These probes help threat actors map Marine Corps networks, potentially exfiltrate data, and otherwise attempt to gain a competitive advantage. Threat actor cyber operations may seek to manipulate Marine Corps information flows and degrade, disrupt, or destroy network information resources.
- The Navy stated that malicious cyber actors could manipulate command-and-control information systems with the intent to degrade decision-making.
- The National Security Agency indicated that any degradation to the information environment might hinder its ability to produce cybersecurity advisories.

Figure 7: Threat Actions in the Information Environment



Source: GAO analysis of Department of Defense (DOD) information; Thaut Images/stock.adobe.com and U.S. Air Force/Staff Sgt. E. Nuñez (photos). | GAO-22-104714

Additionally, several components cited malicious cyber activity against DOD information that is in transit, stored, or at rest in non-DOD systems as a threat to DOD, as illustrated by the following examples.

- NORTHCOM stated malicious cyberspace activities against cleared defense contractors have introduced an ongoing risk to DOD information. Specifically, NORTHCOM stated that China has exfiltrated plans for fighter jet aircraft from a DOD contractor's system. In February 2022, an interagency cyber alert noted that Russian state-sponsored cyber actors had exfiltrated DOD information from cleared defense contractors. The alert noted that this incident granted the actors significant insight into U.S. weapons platforms development and deployment timelines, plans for communications infrastructure, and specific technologies employed by the U.S. government and military.
- TRANSCOM stated that its mission entails working with commercial civilian companies to move cargo and that it must release a substantial amount of sensitive information to these companies. Accordingly, TRANSCOM has become increasingly sensitive to the spillage of sensitive information that could be collected by adversaries. In 2019, the DOD Inspector General issued a report that found that a number of DOD contractors were not complying with a cybersecurity-related defense acquisition regulation focused on protecting DOD information in the defense industrial base.³⁶
- In March 2021, we reported that DOD needs to address multiple cybersecurity challenges to better protect information systems across the department.³⁷ These include protecting financial systems, protecting weapon programs and systems, and addressing department-wide cybersecurity shortfalls in policy and training for personnel. We also continue to designate information security as a government-wide high-risk area in our most recent biennial report to Congress on the federal government's efforts to address information security deficiencies—a designation we have made in each report since 1997.³⁸

"We are facing numerous challenges and aggressive actions fueled by advanced adversary capabilities in cyberspace, space, and electromagnetic spectrum. We can no longer assume information or technical superiority in day-to-day campaigning or combat operations. Additionally, our competitors and adversaries employ propaganda and disinformation to target American citizens, government and military leaders, and military members through global digital communications, media, and social media platforms."

— Jennifer Edgin, Assistant Deputy Commandant for Information, U.S. Marine Corps, U.S. Marine Corps response to GAO leadership questionnaire

Collection of Information or Intelligence Against DOD

The proliferation of devices, ubiquity of data and information, and a culture where people (including DOD service members, employees, contractors, and family members) readily share information with the public fosters an environment where the "collection of information or intelligence to understand DOD components' mission, operations, or personnel" is a real and growing threat.

In some instances, readily available information could adversely affect military missions or safety and security of military personnel. Recognizing this, in July 2020, the Secretary of Defense issued a memorandum highlighting historical examples of poor operations security that led to loss of life and mission failure and emphasizing the importance of operations security in competing with great power competitors that exploit and weaponize information. Whether poor operations security takes the form of careless cyber hygiene, "loose talk" among colleagues, or the willful release of non-public information, the result is the same: unnecessary and increased risk of harm to Americans and missions. (See prior section on Ubiquitous and Malign Information and section on Security.)

Intentionally or unintentionally released information can also be collected and analyzed by foreign intelligence entities to better understand DOD's capabilities and personnel. For example, the Air Force stated that China has compromised a range of U.S. public and private networks containing sensitive service information, including those for various aircraft and communications systems. According to the Air Force, this compromise may enable China to develop solutions against them, while greatly assisting its own defense procurement efforts. Similarly, the Marine Corps stated that intelligence collection has been a threat to personnel as they

³⁶Department of Defense, Inspector General, *Audit of Protection of DOD Controlled Unclassified Information on Contractor-Owned Networks and Systems* (July 23, 2019).

³⁷GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

³⁸See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021) and *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

have been persistently subject to online phishing by adversaries.

Multiple subject matter experts with whom we spoke cited intelligence collection as a significant threat. One of the experts stated that individuals and machines are constantly transmitting data and information about themselves and their activity or inactivity; however, they are unable to control the extent to which others (including adversaries) collect, use, and exploit this information. This massive transmission of data is a significant vulnerability and enables ubiquitous technical surveillance. The *National Counterintelligence Strategy of the United States 2020-2022* similarly notes readily available and advanced cyber and technical surveillance tools offer threat actors a relatively low-cost, efficient, deniable, and high-yield means of accomplishing their goals.³⁹

Influence Threats

The DOD components responding to our questionnaire identified an adversary's attempts to influence as being a threat in the information environment. In particular, 20 components identified attempts to influence policy making or planning efforts, 19 components identified the targeting of the command-and-control decision-making process, and 19 components identified the targeting of service members'/employees' morale or decision-making as concerns, as illustrated by the following examples.

- SOUTHCOM stated that DOD personnel exposure to adversary propaganda and disinformation can influence DOD perceptions and decision-making.
- The Marine Corps stated that Marines are frequently targets of phishing attacks, against both their personal and professional accounts. This includes targeting users through social media and exploiting social networks. It said that actors likely targeting Marines include both nation-states (who seek to undermine their morale) and transnational criminal organizations (seeking financial gain).
- The Navy stated adversaries are targeting or trying to influence service members' or employees' morale or decision-making regarding COVID-19. This includes adversaries like China and Russia pushing misinformation to sow confusion on the health and safety of COVID-19 vaccinations.

Electromagnetic Spectrum Threats

DOD components also identified actions that could undermine capabilities that leverage the EMS (e.g., radios, GPS, and weapon systems). In response to our questionnaire, 19 DOD components identified "malicious use of EMS to degrade or damage DOD capabilities" and 14 components identified "malicious use of EMS to harm DOD component's personnel (including service members and civilian personnel), contractors, or family members." For example:

- The Air Force stated that Russia has invested in satellite jamming platforms targeting low-earth-orbiting and geosynchronous systems. Additionally, the protracted use of commercial and military-grade GPS jammers may hold at-risk the redundancy and availability of dedicated Air Force satellite communication channels on both military and civilian carriers.
- The Air Force cited open-source media reports that described sporadic Russian radio-electronic interference with U.S. and allied manned and unmanned aircraft in Syria and other locations. They continued, stating that advanced Russian fighter craft now employ digital radio-frequency memory jammers that dynamically select specific threats, which can drastically reduce any advantage U.S. fighter aircraft hold.
- DOD components' responses to our questionnaire are corroborated by the 2020 *DOD Electromagnetic Spectrum Superiority Strategy*, which states that global competitors recognize the EMS as a complex maneuver space that factors into a nation's economic prosperity and relative military advantage.⁴⁰ Recognizing U.S. reliance on the EMS, our adversaries have spent 30 years studying, investing, and implementing policies, capabilities, and procedures with the single focus of gaining military advantage over U.S. forces. These adversaries are developing and fielding advanced technology that targets U.S. capabilities across the EMS.
- We testified in March 2021 that Russian electromagnetic warfare forces have been described by the Defense Intelligence Agency as "world class" and that China also has formed new military units and improved capabilities for EMS operations.⁴¹ According to DOD, the U.S. needs to control the EMS to support warfighting functions or it risks losing the battlespace.

³⁹National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States 2020-2022* (Jan. 7, 2020).

⁴⁰DOD, *Department of Defense Electromagnetic Spectrum Superiority Strategy* (October 2020).

⁴¹GAO-21-440T.

Questions for Oversight

- 1 What controls can DOD put in place to enhance the cybersecurity of IT systems and networks owned by DOD contractors and civilian companies that DOD relies on for its operations?
- 2 What actions and training can DOD put in place to educate personnel (including dependents) to understand the operations security or intelligence value of even what may appear to be innocuous postings on social media to protect our personnel and actions?
- 3 What actions can DOD take to prepare and protect service members, civilian employees, and contractors from falling victim to influence campaigns by malicious actors?
- 4 What is DOD's plan to ensure long-term commitment to gain EMS superiority and should DOD consider establishing a structure similar to that used in the cyber domain (e.g., U.S. Cyber Command, U.S. Army Cyber Command, Deputy Principal Information Operations Advisor, J6, A6)?

Table 3 shows how DOD components identified actions they consider to be a threat to their organization in the information environment in their responses to our questionnaire.

Table 3: DOD Component Responses to Information Environment Threats

| Threat action | Yes | No | Unknown | Top five most important |
|---|-----|----|---------|-------------------------|
| Malicious cyber activity against component information systems | 24 | 0 | 1 | 23 |
| Actions to implant, modify, destroy, or extract data within component information systems | 24 | 0 | 1 | 20 |
| Collection of information or intelligence to understand component's mission, operations, or personnel | 22 | 1 | 2 | 18 |
| Target or try to influence policy making or planning efforts | 20 | 4 | 1 | 12 |
| Physical attacks against component information systems | 20 | 3 | 2 | 4 |
| Target or try to influence commander's/leader's command-and-control decision-making process | 19 | 4 | 2 | 8 |
| Malicious use of the EMS to degrade or damage capabilities | 19 | 3 | 3 | 7 |
| Physical attacks against component electromagnetic spectrum (EMS) capabilities | 19 | 4 | 2 | 5 |
| Target or try to influence service members' or employees' morale or decision-making | 19 | 2 | 4 | 4 |
| Physical attacks against component personnel (including service members and civilian personnel), contractors, or family members | 16 | 3 | 6 | 2 |
| Malicious use of EMS to harm component personnel (including service members and civilian personnel), contractors, or family members | 14 | 4 | 7 | 3 |
| Other threat actions | 1 | 0 | 0 | 0 |

Source: GAO analysis of Department of Defense (DOD) components' responses to GAO's questionnaires. | GAO-22-104714

Note: In our questionnaire, we asked DOD components to identify actions that pose a threat to their organization in the information environment, and which five of those identified actions that they consider to be most important. The "Top Five" column here notes that a component selected the threat actor as one of its most important. We used the term "most important" in the questionnaire sent to all 25 DOD components. We let each DOD component use its own reasoning and understanding to guide responses and interpretation of what constituted something as "most important."



Institutional Challenges for DOD Related to the Information Environment

National and departmental strategies recognize that DOD faces a number of institutional challenges—including a lack of leadership emphasis, lack of resources, the implications of new technology, and dated processes—that need to be addressed. The 25 DOD components who responded to our questionnaires similarly highlighted disparate institutional challenges.

We asked 25 DOD components to select issue areas that they consider to be a challenge to their organization in the information environment. In our questionnaire, we provided the DOD components with 14 response options, as seen in figure 8, and an opportunity to write in others. We then asked the components to identify the five challenges they consider to be most important.⁴² Below are anecdotal examples that DOD components identified in their component questionnaires that illustrate institutional challenges cited as most important—personnel, funding, information technology, organization, and training.

Figure 8: Institutional Challenges for DOD Related to the Information Environment



Source: GAO. | GAO-22-104714

Personnel-Related Challenges

Overall, 21 of 25 components identified personnel-related challenges—such as having personnel with inadequate expertise or insufficient numbers of personnel—as an information environment-related institutional challenge. Thirteen of these 21 components consider personnel as one of their five most important institutional challenges in the information environment, as illustrated by the following examples.

- SOUTHCOM and SPACECOM, acknowledged that having sufficient numbers of personnel is an institutional challenge. SPACECOM, in an amplifying narrative, stated that the command requires a full complement of personnel to accomplish activities associated to each information-related capability to enable the command to maintain digital superiority, promote responsible behaviors in space, and unite the space community around a compelling narrative.⁴³ Similarly, the Defense Digital Service stated that insufficient numbers of technology specialists throughout the department—encompassing software and infrastructure engineers, technical product managers, user experience designers, and data scientists—makes it difficult for the agency to support software development.
- The Air Force stated that it experienced challenges retaining adequate numbers of personnel with needed expertise. For example, until the service established a career field for information operations in 2016, service members from various career fields served in information operations positions for a limited period. Because these service members then returned to their primary career fields, the Air Force was limited in its ability to sustain institutional knowledge and practice of information operations tactics, techniques and procedures.

In August 2019, we reported that rising threats posed by great-power competitors, particularly China and Russia, have prompted the Army to undertake substantial changes to how it operates and has included the accelerated creation of new cyber and

⁴²We used the term “most important” in the questionnaire sent to all 25 DOD components. We let each DOD component use its own reasoning and understanding to guide responses and interpretation of what constituted something as “most important.”

⁴³An information-related capability is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials.

electronic warfare units.⁴⁴ However, we found that these units were not fully staffed. Furthermore, we found that the Army had established these units without completely assessing the staffing (and equipping and training) risk to those units over the long term, leaving senior Army leaders with an incomplete picture of the challenges in affording, supporting, and sustaining these units. We made recommendations related to assessing risks for staffing, equipping, and training units. The Army addressed all of these.

"Russia possesses a robust information force while China continues to evolve and improve. The United States' principal disadvantage is the lack of ample information force at all levels—it lacks a deep bench."

— GAO Interview with Mr. Michael Schwillie, Senior Policy Analyst, RAND Corporation

Funding-Related Challenges

Overall, 20 of 25 components identified inadequate, insufficient, or misprioritized funding as an information environment-related institutional challenge. Thirteen of the 20 DOD components consider funding as one of their five most important institutional challenges in the information environment. For example, AFRICOM, INDOPACOM, and SOUTHCOM, asserted they do not have adequate resources to perform missions in the information environment. AFRICOM stated the current deficiency limits its ability to develop the means to assess and measure the effectiveness of activities undertaken in the information environment. In October 2019, we found that DOD had made limited progress in implementing its 2016 Information Operations strategy because the department had not developed an implementation plan or an investment framework to identify planning priorities to address information operation gaps.⁴⁵ We made recommendations related to clearly defining roles and responsibilities, issuing policy identifying formal responsibilities for providing oversight, and establishing a process that facilitates implementation. DOD continues to work toward implementation of these recommendations.

Information Technology-Related Challenges

Overall, 20 of 25 components identified inadequate, insufficient, and outdated information technology as an information environment-related institutional challenge. Thirteen of the 20 DOD components consider information technology as one of their five most important institutional challenges in the information environment, as illustrated by the following examples.

⁴⁴GAO, *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*, GAO-19-570 (Washington, D.C.: Aug. 15, 2019).

⁴⁵GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019). We reiterated this finding in our April 2021 testimony (GAO-21-525T).

- NORTHCOM said that systems required to collect, process, analyze, and display information to decision makers require modernization, additional bandwidth, and may require different power and cooling requirements. In addition, NORTHCOM stated it requires upgraded information capabilities enabled by artificial intelligence to achieve multi-domain awareness.
- DISA stated that establishing a common data standard and exchange in the information environment is a challenge due to a long history of managing services and systems that were primarily independent and not integrated well. DISA continued that it is moving toward common data sources and integration, but this takes time and funds.
- The Navy stated that the proliferation of data from unmanned systems has made the continued tasking, collection, processing, exploitation and dissemination of intelligence a challenge.

Organization-Related Challenges

Overall, 18 of 25 components identified issues pertaining to how they are organized as being an information environment-related challenge. Ten of the 18 DOD components consider Organization as one of their five most important institutional challenges in the information environment, as illustrated by the following examples.

- The Navy stated that the service does not have a central and coherent management of its informational activities to inform, influence, persuade, and defend Navy informational activities in and through the information environment at the leadership level.
- Space Force stated that while the service was designed to be mission-focused by being a flat organization that leverages digital processes, it has to work through a broader DOD structure that was mostly developed during the industrial-age.

Training-Related Challenges

Overall, 23 of 25 components identified inadequate, insufficient, or outdated training as an information environment-related institutional challenge. Nine of the 23 DOD components consider training as one of their five most important institutional challenges in the information environment, as illustrated by the following examples.

- The Defense Media Activity acknowledged training as a challenge. It stated that its Defense Information School will continue to work with the military services to ensure that the curriculum for both Public Affairs and Visual Information aligns with their requirements and prepares graduates to operate effectively in the information environment.
- The Office of the Secretary of Defense stated that training for its personnel and leadership related to the information environment and IT systems are limited.

Questions for Oversight

- 1 To what extent has the Department of Defense established a comprehensive plan identifying information environment-related personnel requirements and how to fulfill them?
- 2 To what extent does the Department of Defense have visibility on the budgetary resources presently allocated for information environment requirements?
- 3 To what extent has the Department of Defense established a comprehensive plan identifying information environment-related IT requirements and how to fulfill them?

Table 4 shows how DOD components identified issue areas that they consider to be a challenge to their organization in the information environment in their responses to our questionnaire.

Table 4: DOD Component Responses to Information Environment-Related Institutional Challenges

| Area | Yes | No | Unknown | Not applicable | Top five most important |
|--------------------------|-----|----|---------|----------------|-------------------------|
| Training | 23 | 1 | 1 | 9 | 16 |
| Personnel | 21 | 2 | 2 | 13 | 11 |
| Funding | 20 | 3 | 2 | 13 | 5 |
| Information technology | 20 | 4 | 1 | 13 | 12 |
| Policy | 20 | 3 | 2 | 8 | 10 |
| Organization | 18 | 6 | 1 | 10 | 9 |
| Data information | 17 | 5 | 2 | 8 | 4 |
| Facilities | 17 | 4 | 4 | 4 | 0 |
| Materiel | 17 | 5 | 3 | 4 | 18 |
| Interagency coordination | 15 | 7 | 2 | 6 | 15 |
| Coordination with allies | 14 | 9 | 2 | 5 | 3 |
| Plans | 14 | 8 | 3 | 2 | 3 |
| Doctrine | 13 | 9 | 3 | 3 | 2 |
| Leadership | 13 | 8 | 3 | 3 | 3 |
| Other | 1 | 0 | 0 | 1 | 1 |

Source: GAO analysis of Department of Defense (DOD) components' responses to GAO's questionnaires. | GAO-22-104714

Note: In our questionnaire, we asked DOD components to identify issue areas that they consider to be a challenge to their organization in the information environment, and which five of those identified challenges that they consider to be most important. The "Top Five" column here notes that a component selected the challenge area as one of its most important. We used the term "most important" in the questionnaire sent to all 25 DOD components. We let each DOD component use its own reasoning and understanding to guide responses and interpretation of what constituted something as "most important."



Emerging Technologies Associated with the Information Environment

A number of emerging technologies have the potential to accelerate change and introduce both opportunities for—and threats to—DOD in the information environment. During our review, we asked DOD components to identify emerging technologies that they consider to present either a threat to or an opportunity for their organization in the information environment. The DOD components identified a variety of technologies—such as artificial intelligence (AI) and machine learning, quantum computing, social media platforms, deepfakes, and bots—that could have either a positive or negative effect on DOD in the information environment.

In addition to those technologies, reports we reviewed and subject-matter experts with whom we met identified extended reality, fifth-generation (5G) wireless telecommunications, and Internet of Things (IoT) as technologies that have both positive benefits and negative consequences. These technologies can affect decision-making and perceptions of a situation. What follows are descriptions of selected emerging technologies based on the DOD component questionnaires, literature review, and our prior work.

Artificial Intelligence

While there are various definitions of AI, in general, AI refers to computer systems that are able to solve problems and perform tasks that have traditionally required human intelligence and that continually get better at their assigned tasks. In February 2022, we reported that DOD identified a variety of potential warfighting and non-warfighting uses for AI across the department.⁴⁶

DOD’s potential AI uses in warfighting operations include analyzing intelligence, surveillance, and reconnaissance sources; fusing data to provide a common operating picture on the battlefield; supporting semiautonomous and autonomous vehicles; and operating lethal autonomous weapon systems. Potential non-warfighting uses for AI (i.e., support and business operations) include resolving unmatched financial transactions, predicting maintenance needs, vetting security clearances, and analyzing warfighter health screenings. In June 2021, we issued an accountability framework for federal

government managers to help ensure responsible use of AI in government programs and processes.⁴⁷

In answering our information environment questions, DOD components identified additional threats and opportunities that may result from continued development of AI, as shown in table 5.

Table 5: Selected Examples of Opportunities and Threats Posed by Artificial Intelligence (AI), as Identified by DOD Components



- » **Opportunities:** The Marine Corps, U.S. Northern Command, U.S. Space Command, and U.S. Transportation Command cited the potential for AI to enhance DOD decision-making and activities. Specifically, the Marine Corps stated that AI/machine learning can support decision-making by aggregating and parsing large swaths of data faster and more accurately than humans. Additionally, the Defense Information Systems Agency, the Office of the Secretary of Defense, and U.S. Southern Command noted the potential for AI to be used in analysis of threats to DOD in the information environment.
- » **Threats:** The Air Force said that ongoing research and development in AI applications by adversaries will introduce qualitative improvements to Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (known within DOD as C4ISR) systems and the overall performance of unmanned aerial vehicles and missiles. The Air Force added that China views AI as a rare opportunity to step out in front of the United States in high-technology applications, and is making tremendous investments in AI research. According to the Marine Corps, their adversaries’ ability to leverage machine learning and potentially AI to process publicly available information in support of targeting efforts is a threat to DOD interests.

Source: GAO analysis of DOD components’ responses to GAO’s questionnaires; pickup/stock.adobe.com (photo). | GAO-22-104714

In our December 2018 report identifying emerging threats to national security, we reported that 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.⁴⁸ In March 2021, the National Security Commission on Artificial Intelligence issued its final report in which the commission

⁴⁶GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, GAO-22-104765 (Washington, D.C.: Feb. 17, 2022).

⁴⁷GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, GAO-21-519SP (Washington, D.C.: June 30, 2021).

⁴⁸GAO-19-204SP.

described additional cybersecurity risks associated with AI and recommendations to address them.⁴⁹ Specifically, the commission stated that AI will enable malware to mutate into thousands of different forms, find vulnerabilities, and attack selectively. The commission added that the expanding application of AI cyber capabilities will make cyberattacks more precise and tailored; further accelerate and automate cyber warfare; enable stealthier and more persistent cyber weapons; and make cyber campaigns more effective on a larger scale.

Also in March 2021, we provided an update on progress federal agencies have made in addressing major cybersecurity challenges.⁵⁰ In that report, we noted that AI holds substantial opportunity in a variety of capacities. Using AI to automate computer network defense offers many potential gains in terms of efficiency and effectiveness. For example, AI automated systems and algorithms can help identify and patch vulnerabilities and defend against attacks.

However, AI also poses unique challenges. Automated systems themselves are susceptible to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly identify. These threats are amplified by the ongoing delegation of decision-making, sensing, and authentication roles to potentially vulnerable automated systems. Moreover, broader deployment could become riskier as the reliance on autonomous decision-making increases. As cybersecurity threats enabled by artificial intelligence have the potential to become more effective, it is all the more important for DOD and the rest of the federal government to improve the implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents.

In March 2022, we found that the department's AI-related strategies could be more comprehensive—such as by including full descriptions of the resources needed—and that DOD had not yet issued guidance clearly defining the roles and responsibilities of components that participate in AI activities.⁵¹ We made seven recommendations to address these and other issues.

Quantum Technologies

Quantum technologies build on the study of the smallest particles of energy and matter to collect,

generate, and process information in ways not achievable with existing technologies. Quantum sensors could be used in science, industry, and navigation to make more precise and accurate measurements and offer potential benefits for critical defense and civilian applications, including maintaining timing and position accuracy in GPS-challenged or denied environments. Quantum communications could allow businesses and governments to securely transmit information. Quantum computers could dramatically accelerate computation for some applications, such as machine learning and decrypting information.

In answering our information environment questions, DOD components identified additional opportunities and threats that may result from continued development of quantum technologies, as shown in table 6.

Table 6: Selected Examples of Opportunities and Threats Posed by Quantum Technologies, as Identified by DOD Components



» **Opportunities:** U.S. Space Command stated that quantum computing provides significantly increased processing power and communications speed, as well as the opportunity to better secure systems. The Air Force noted that quantum computing may enhance resource portfolio management, enable rapid detection of malign foreign influence, and support algorithmic warfare.

» **Threats:** U.S. Space Force and the Marine Corps noted that quantum computing has the potential to threaten or render current encryption methods obsolete. The Air Force stated that quantum sensors could enable adversaries to operate in GPS-degraded environments as well as more effectively detect submarines, underground structures, and electromagnetic signals.

Source: GAO analysis of DOD components' responses to GAO's questionnaires; AndSus/stock.adobe.com (photo). | GAO-22-104714

In a 2021 technology assessment about quantum computing and communications, we reported that quantum information technologies could dramatically increase capabilities beyond what is possible with classical technologies.⁵² Future quantum computers

⁴⁹Section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the National Security Commission on Artificial Intelligence as an independent commission to consider the methods and means necessary to advance the development of AI, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States. Pub. L. No. 115-232, § 1051, (2018). National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

⁵⁰GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

⁵¹GAO, *Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance*, GAO-22-105834 (Washington, D.C.: Mar. 30, 2022).

⁵²GAO, *Technology Assessment: Quantum Computing and Communications: Status and Prospects*, GAO-22-104422 (Washington: D.C.: Oct. 19, 2021).

could have high-value applications in security and cryptography. Future quantum communications could allow for secure communications by making information challenging to intercept without the eavesdropper being detected, quantum networking, and a future quantum internet.

In May 2020, we reported that quantum computing has the potential to create major cybersecurity risks.⁵³ For example, a full-scale quantum computer has the potential to break standard encryption technologies, creating a major information security risk. As a result, the federal government's cybersecurity infrastructure will need to evolve to address this threat. Conversely, our December 2018 report on emerging threats to national security noted that quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt.⁵⁴ Quantum computing may allow adversaries to decrypt information, which could enable them to target U.S. personnel and military operations.

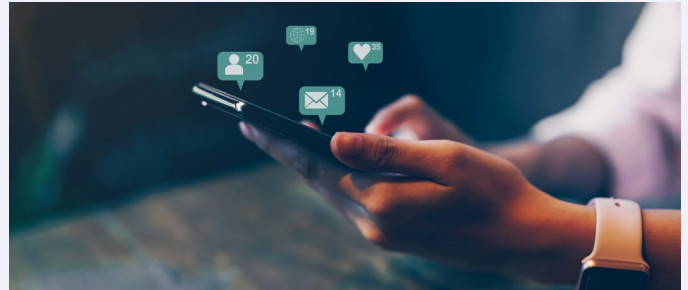
The Cyberspace Solarium Commission has also highlighted the cybersecurity challenges related to quantum computing. In particular, the commission recommended that Congress require DOD to comprehensively assess the threats and risks posed by quantum computing to national security systems and develop a plan to secure those systems.⁵⁵ Subsequently, in January 2021, Congress included a provision in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 that required the Secretary of Defense to prepare such an assessment and to develop recommendations for research, development, and acquisition activities for securing critical national security systems against threats to quantum computing.⁵⁶

Social Media Platforms

Social media platforms enable users to do the following: create individual profiles; form networks; produce content by posting text, images, or videos; and interact with content by commenting on and sharing it with others. Two attributes of social media platforms—the user networks and the algorithmic filtering used to govern the sharing content—can contribute to the spread of misinformation. Users can build their own social networks, which affect the content that they see, including misinformation. Most social media operators use algorithms to sort and prioritize the content placed on their sites; such algorithms are generally built to increase user

engagement, but they can amplify the distribution of certain content, which can include misinformation.⁵⁷ In answering our information environment questions, DOD components identified additional threats and opportunities that may result from social media platforms, as shown in table 7.

Table 7: Selected Examples of Opportunities and Threats Posed by Social Media Platforms, as Identified by DOD



» **Opportunities:** U.S. Africa Command (AFRICOM), the Joint Information Operations Warfare Center (JIOWC), the Navy, U.S. Northern Command (NORTHCOM), U.S. Southern Command (SOUTHCOM), and U.S. Space Command (SPACECOM) identified social media as a technology that could be used to promote Department of Defense (DOD) information, counter adversaries' messaging, or collect data to inform decision-making. For example, NORTHCOM stated that it uses social media to coordinate DOD messaging with other federal agencies. The JIOWC stated that social media creates opportunities to disrupt adversary actions and operations. SOUTHCOM stated that AI-enabled social media analysis has been a huge asset in analyzing large data sets.

» **Threats:** The ability for adversaries to use social media to spread misinformation and disinformation to potentially deceive U.S. audiences, service members, and allied military and civilian populations was noted by AFRICOM, the Army, the Defense Information Systems Agency, Joint Staff, JIOWC, the Marine Corps, NORTHCOM, SOUTHCOM, SPACECOM and U.S. Transportation Command.

AFRICOM stated that social media has increased adversary access to audiences and enabled disinformation campaigns. They added that current (younger and upcoming) adversaries have a greater general familiarity with IT, social media-specific training, and more latitude to exercise initiative in the social media information environment, which increases the level of threat to AFRICOM's objectives.

The Marine Corps highlighted the threat of social media to its own personnel, stating that adversaries' ability to intrude in the social network communities of Marines and conduct misinformation/disinformation campaigns can potentially affect Marines' commitment to a mission if incorrect information is present at high rates and seems legitimate.

Source: GAO analysis of DOD components' responses to GAO's questionnaires; sitthiphong/stock.adobe.com (photo). | GAO-22-104714

Deepfakes

Deepfakes—an AI-enabled technology that can be used to replace faces, manipulate facial expressions, synthesize faces, and synthesize speech in video, photo, or audio recordings—are powerful tools that can be used for exploitation and disinformation. In

⁵³GAO, *Science & Tech Spotlight: Quantum Technologies*, GAO-20-527SP (Washington, D.C.: May 28, 2020).

⁵⁴GAO-19-204SP.

⁵⁵U.S. Cyberspace Solarium Commission report; Washington, DC: March 2020. <https://www.solarium.gov/report>.

⁵⁶Pub. L. No. 116-283, § 1722, (2021).

⁵⁷CRS, *Social Media: Misinformation and Content Moderation Issues for Congress*, R46662 (Washington, D.C.: Jan. 27, 2021).

2020, we issued a science and technology spotlight that highlighted that deepfakes could be used to influence elections or incite civil unrest, or as a weapon of psychological warfare. Deepfakes could also lead audiences to disregard legitimate evidence of wrongdoing and, more generally, undermine public trust in audiovisual content.⁵⁸

The Navy, the Office of the Secretary of Defense, SPACECOM, and Space Force also cited deepfakes as a technology that has the potential to sway public opinion or undermine U.S., allied, or partner credibility. For example, Space Force stated that an adversary could use deepfakes to inject false or misleading information into its decision-making processes. Space Force also said that deepfakes could be used to spread seemingly credible disinformation about its operations or capabilities into the public awareness that it would have to actively work to correct, wasting resources while giving adversaries time to maneuver.

Bots

Bots are lines of computer instructions that work to execute tasks autonomously and repetitively. For example, they simulate the behavior of human beings in a social network: interact with other users, and share information and messages. Based on the way that the bots are developed, they can learn from response patterns or input values to respond to certain situations (i.e., they possess AI capabilities). Using these capabilities, the bots simulate users' behavior, which could include the propagation of misinformation and disinformation. NORTHCOM and SOUTHCOM cited the hostile use of "bots," programs that imitate legitimate user activities, on social media platforms in spreading malign information, such as voter safety in the 2020 national elections.

Fifth-Generation (5G) Wireless Communications

Fifth-generation (5G) wireless networks promise to provide significantly greater speeds; higher capacity to accommodate more devices; and are expected to be more flexible, reliable, and secure than existing cellular networks.⁵⁹ At the same time, we have identified challenges that can hinder the performance or usage of 5G technologies in the U.S. For example, spectrum demand will likely continue to exceed supply; and 5G networks will likely exacerbate privacy concerns, perpetuate concerns about the supply chain for network components, and potentially introduce new modes of cyberattack and expand the potential points of attack.

Extended Reality Technologies

Extended reality is the overarching term for a spectrum of technologies that link or integrate the digital world and the real world. These include augmented reality, mixed reality, and virtual reality technologies, all of which provide different degrees of sensory immersion and interaction between the real world and digital content. Augmented reality overlays digital content onto representations of the real environment, using smartphones, tablets, or augmented reality glasses. In mixed reality, a dedicated headset recognizes its environment and enables the interaction between digital content and the real world in multiple dimensions. Virtual reality completely obscures the real world, immersing users in digital environments using head-mounted displays.

In 2022, we reported that extended reality technologies provide a number of opportunities.⁶⁰ For example, the technologies could provide data sharing and digital workspaces that support collaborative planning and decision-making (such as those conducted for military operations), analyzing data in extended reality environments might allow new kinds of knowledge generation or decision-making, and expensive or dangerous procedures (such as large-scale military training) might be taught more cheaply and safely in extended reality environments.

However, we have reported and public articles highlight challenges and risks—such as those associated with

- cybersecurity;
- privacy;
- bandwidth limitations;
- the underlying data being vulnerable to bias and misuse;
- effects on users; and
- information captured by these technologies that track our feelings, judgments, reactions and broader sets of traits that make us who we are (i.e., information that could be used against military personnel conducting military operations).

Internet of Things

The IoT is the set of internet-capable devices, such as wearable fitness devices and smartphones that interact with the physical environment, and typically contain elements for sensing, communicating, processing, and actuating. The Defense Digital

⁵⁸GAO, *Science and Tech Spotlight: Deepfakes*, GAO-20-379SP (Washington, D.C.: Feb. 20, 2020).

⁵⁹GAO, *Technology Assessment: 5G Wireless Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: Nov. 24, 2020); and *Science & Tech Spotlight: 5G Wireless*, GAO-20-412SP (Washington, D.C.: Mar. 26, 2020).

⁶⁰GAO, *Science & Tech Spotlight: Extended Reality Technologies*, GAO-22-105541 (Washington, D.C.: Jan. 26, 2022).

Service stated that the IoT provides it with a framework for thinking about its efforts to connect sensors with situational awareness and command-and-control tools. However, the National Security Agency commented that IoT technologies, particularly smart medical devices are an operations security concern.

Consistent with the National Security Agency’s comment, we previously reported that DOD documents and officials identified numerous security risks with IoT devices—as highlighted in table 8—that can generally be divided into risks with the devices themselves and risks with the devices’ operational implications.⁶¹

Table 8: Internet of Things (IoT) Security Risks Identified by Department of Defense (DOD)



| Risks | | Description of concern |
|-------------------|---|---|
| Device risks | Supply chain threat | The manufacturing origin of IoT devices and related components. Adversaries like China and Russia could embed “exploits,” or malicious software, into the hardware of chips and other components used in IoT devices, such as smart meters, to collect and transmit data. |
| | Limited encryption | Limited encryption in IoT hardware or the collection and transmission of unencrypted data. IoT devices have not been designed to facilitate deployment of the latest cryptographic algorithms and protocols, thus posing a range of potential risks, to include eavesdropping, unauthorized access, and device tampering. |
| | Poor security in device design | Current IoT devices have limited security in the design of their hardware and software, including chip design and cybersecurity software. With little built-in security, IoT devices could be compromised without the user’s knowledge. |
| | Poor password management or authentication | Poor password management or authentication protocols could lead to DOD industrial control systems or personal IoT accounts being compromised or manipulated by hackers. |
| | Patch or upgrade deficiencies | As the number of IoT devices increases, the probability of missing—or not implementing—a security upgrade or patch increases. Further, some devices may not be patchable at all. In addition, a device could be kept in service longer than it is scheduled to receive security or management updates, which at least one DOD component refers to as a “zombie device. Any of these situations could lead to potentially vulnerable or exploitable devices by which adversaries could gain unauthorized access. |
| Operational risks | Rogue applications ^a | Some device applications—such as gaming applications—could be installed on personal or even DOD smartphones or other devices, which then take pictures or record the user’s locations. Such functionality could pose security risks for DOD personnel or facilities. |
| | Adverse impacts of devices on operations security ^b | IoT devices, including personal smartphones, can tag a person’s location—known as geo-tagging—which presents implications for operations security. Officials from three services noted the lack of awareness among their personnel over IoT device capabilities in their environment and the need for behavioral changes. |
| | Rogue wireless devices ^a and insider threat ^c | An increase in the number of IoT devices could significantly increase DOD’s vulnerability to cyber collection. Rogue wireless devices planted by an insider threat or intentionally placed by service personnel (and then compromised) could collect sensitive information or send out data on industrial control systems for purposes of espionage. |
| | Expansion of attack surface | The expansion of IoT devices will significantly increase the number of points at which any network can be attacked. IoT devices would provide more attack vectors into a network and a potential platform for massive, distributed attacks. |
| | Unauthorized communication of information to third parties | Some IoT devices could by design collect and send data back to commercial providers, such as third-party help desks, and DOD components may have little insight into the internet destinations of such data. |

Source: GAO analysis of DOD information; metamorworks/stock.adobe.com (photo). | GAO-22-104714

Note: This table may not identify all of DOD’s IoT security risks, but is intended to capture key risks cited by DOD—including the Defense Science Board, the DOD Chief Information Officer, the Defense Intelligence Agency, and the Joint Staff. We also interviewed several non-DOD organizations to corroborate and discuss IoT security concerns, including the Internet Society, the National Institute of Standards and Technology, and the Office of the Director of National Intelligence. They generally reinforced the security risks in the table.

^aDOD officials use the term “rogue” in referring to applications and wireless devices that could be used for malicious purposes even though the applications or wireless devices by themselves are not malicious in nature.

^bDOD defines operations security in part as a process of identifying critical information and analyzing friendly actions to identify those actions that can be observed by adversary intelligence systems, determine vulnerabilities that these adversary systems might obtain that could be pieced together to derive critical information, determine which of these represent an unacceptable risk, and then select countermeasures to eliminate or reduce the risk to friendly actions.

^cInsider threats can include DOD personnel working directly with adversaries to collect information or DOD personnel unintentionally assisting adversaries through their inattention to cybersecurity or other actions.

⁶¹GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

Questions for Oversight

- 1 How is DOD positioned to counter the use of AI-enabled capabilities for cyberattacks, espionage, and psychological or political warfare below the threshold of direct military confrontation by state and non-state adversaries?
- 2 What are the national security implications of other nations developing quantum technologies? What are the implications of adversaries using quantum computing being able to break present-day encryption schemes?
- 3 What are the national security implications of adversaries developing quantum sensor technologies that could potentially defeat U.S. stealth capabilities?



Past and Planned Actions to Use or Protect the Information Environment

DOD has recognized that the department needs to transition into an information-age era. Among other things, it established “information” as a joint function in 2017, issued the *Joint Concept for Operating in the Information Environment* in 2018, and drafted Joint Publication 3-04, which, according to JIOWC officials, is expected to be issued in 2022. Furthermore, achieving and sustaining an advantage requires DOD to undertake and plan actions across multiple areas, including doctrine, organization, and training.

During our review, we asked DOD components to identify

- actions that they have undertaken to use or protect the information environment for the time period from October 2018 (after Information was identified as a joint function in joint doctrine in 2017) to the fall of 2021;⁶² and
- actions they plan to undertake to use or protect the information environment from the fall of 2021 to the end of September 2023.

In our questionnaire, we provided DOD components with 11 response options and an opportunity to write in others for actions the components had taken as well as those actions it planned on taking. More than 50 percent of DOD components acknowledged taking or planning to take actions for each of these 11 options. Below are anecdotal examples of those options.

Doctrine

The Joint Staff plans to issue a new joint doctrine publication, Joint Publication 3-04, *Information in Joint Operations*, with the intention of reframing the intellectual approach for how DOD considers operations in the information environment and revise the definitions of “information environment” and related terms. This joint publication, according to DOD officials, will establish strategic-level doctrine and lexicon that the Joint Staff will use when describing information environment-related concepts; however, the officials acknowledged that the department as a whole and DOD components will still need to synchronize their policies, doctrines, and lexicon. Other DOD components, such as the Army, Marine Corps, and Air Force, are in the process of

updating related doctrine or have done so since 2018.

Organization

In 2017, the Marine Corps established the Office of the Deputy Commandant of Information to develop and supervise plans, policies, and strategy for operating in the information environment and identify requirements in doctrine, manpower, training, education, and equipment to support Marine Air Ground Task Force operations. In 2022, the Secretary of Defense established the Office of Information Operations Policy, identified a general officer to serve as the department’s Deputy Principal Information Operations Advisor, and established an Information Operations Cross Functional Team.

Training

The Joint Information Operations Warfare Center stated it has developed computer-based training that all DOD organizations could use. The class covers influence awareness and introduces the user to influence objectives and goals; the characteristics and tools of influence; and the threat and examples of influence operations.

The Air Force, Army, and Space Force also described their plans for training. The Air Force stated, over the near term, the Information Operations Field Training Unit will increase its focus on the information environment. Specifically, the unit will, in fiscal year 2022, combine the Air Force Operations Security Course and the Operational Military Deception Course to form a new Air Force Denial and Deception Course that broadens the application of deception and signature management at the tactical and operational level. In fiscal year 2023, the unit will start to develop a new Air Component Influence Course, which will be advanced training customized for Air Force Information Operations officers and air component planners.

The Army reported its training efforts include increased integration of information activities and threat information capabilities in simulations and war games, as well as integration at the Army Combat Training Centers. Lastly, the Space Force stated it had created a program to train and track Guardians as software coders to facilitate innovation at the tactical level via digital applications.⁶³

⁶²We sent our questionnaire to the DOD components in August 2021. Responses were received back from September to December 2021.

⁶³The U.S. Space Force term “Guardians” refers to military personnel in that service. It is analogous to “Soldier,” “Sailor,” “Airman,” or “Marine” for the other military services.

Command Exercises

The JIOWC reported that it has been working with the Joint Staff and combatant commands on command post and tabletop exercises regarding the Information function. According to the Air Force's response, it sponsored two information warfare tabletop exercises—Information Warfare Senior Leader Summits—that identified several major lessons learned, including the need for the service to appoint a lead organization to develop and publish strategic information warfare policy.

Field Exercises

Multiple DOD components highlighted past, ongoing, and planned future exercises.

- SPACECOM stated it has led key multinational activities to improve its mission and synchronize efforts with our allies and partners (including Japan and Australia) and will continue to do so into the future.
- NORTHCOM described its Global Information Dominance Experiment initiative, which aims to improve cross-command and interagency information sharing using cloud computing. NORTHCOM conducted three experiments in the series: December 2020, March 2021; and July 2021. Going forward, NORTHCOM stated it would participate in the Globally Integrated Exercise series with the Joint Staff and multiple combatant commands.
- The Defense Information Systems Agency stated it plans to continue conducting various exercises to include the testing of its Continuity of Operations capability as well as various classified operational exercises testing its ability to react to nation-state supported threats.
- The Marine Corps conducted an 11-day warfighting exercise in May 2021 that was comprised of more than 8,000 combined participants.⁶⁴ Competition in the information environment was a key component of the exercise, in which commands and staffs experimented with evolving technologies and tactics. At the same time, units learned how to better manage spectrum signatures, organize command-and-control systems to further enable assured communications, and improve interoperability with aviation, logistics, and combat service support capabilities.

Materiel

NORTHCOM has invested in information technology systems that are to allow the command to transition

from local workstation computers and on-site servers to virtual desktop interface workstations and cloud-computing data management.

Leadership

Multiple DOD components highlighted past, ongoing, and planned changes to leadership responsible for the information environment.

- In 2020, the Secretary of Defense designated the Under Secretary of Defense for Policy as DOD's Principal Information Operations Advisor. To execute the responsibilities on a daily basis, the Secretary of Defense indicated he intended to select a full-time general-officer, flag-officer, or senior executive to serve as the Deputy Principal Information Operations Advisor.
- The Space Force designated an official at the senior executive service level to serve as the Chief for the service's Technology and Innovation Office to oversee an office that combines science and technology, digital transformation, enterprise information technology requirements, data management, and analysis. This office is to drive innovation, inject technology, and maintain a competitive advantage over potential adversaries.
- In 2020, DARPA issued a memorandum entitled "Appointment Updates for Cybersecurity and Cyberspace Operations Roles", which explicitly identified cyberspace operational roles for specific leaders—an action that the agency stated was a marked change and reflection of senior leadership being fully engaged on cyberspace management.

Facilities

TRANSCOM has incorporated additional security features at its facilities, including installing cell phone monitoring and detection devices, and having security assessments conducted by the Defense Threat Reduction Agency. NORTHCOM and Space Force identified actions that they were taking within existing facilities to increase the ability of personnel to conduct work at a higher classification levels. For 2022, DARPA plans to adapt physical layouts and upgrade security and communications capabilities to support modeling and simulation and multilevel security demonstrations. This will create new capabilities for the associated personnel and mission systems in the information environment.

Personnel

The Marine Corps redesignated its cyber operations career field to an Information Maneuver career field. This new career field allows the service to formally manage the career path of Marines with

⁶⁴A warfighting exercise is designed to pit an exercise force against an adversary force and to replicate the challenges of peer-to-peer competition in the context of emerging operational concepts.

highly specialized training required for space, electromagnetic spectrum operations, cyber warfare, civil affairs, and psychological operations. Similarly, as mentioned above, the Air Force established its Information Operations Officer career field.

Policy

The Air Force is updating the services policy and guidance documents associated with operations security, information operations, and electromagnetic warfare. In 2019, DARPA issued a cyberspace-related policy.

Plans

SPACECOM is updating its campaign and contingency plans to include information-related tasks and integration through the information warfare directorate. These plans will provide guidance for information-related capability implementation in support of SPACECOM missions.

The mission is to provide information, path ways for information and deny information to adversaries. If you think about what we do in space, it's those three things, what we do in cyber is those three things. ... To do those three things, you have to be able to control those domains and when you can't, you have a significant challenge, so to figure out how to expand the space, how to aggregate your capabilities in order to be lethal, disaggregate in order to survive. Those kind of structures were not in the first iteration of the [October] war fighting concept [wargame] and that's why it failed.

— then-General John E. Hyten, Vice Chairman of the Joint Chiefs of Staff, remarks at the Emerging Technologies Institute, July 26, 2021

Other Actions

In addition to the options we identified, our review of DOD documents and interviews with DOD officials and subject matter experts identified other actions that the department has taken, has underway, or plans to take in the next 2 years. For example, DOD officials told us that the Office of Information Operations Policy is undertaking an information operations posture review and will use the results from that review to update its 2016 DOD Operations in the Information Environment Strategy. The Under Secretary of Defense for Intelligence and Security established the Applied Research Laboratory for Intelligence and Security in 2018 to better understand topics, such as cognitive security. According to the Applied Research Laboratory for Intelligence and Security, cognitive security is the field of online and offline influence—and protection from influence—of individuals and large populations.

Questions for Oversight

- 1 To what extent has the Department of Defense established a plan outlining the priorities for use and protection of the information environment?
- 2 To what extent has the Department of Defense established a plan outlining the priorities for training and exercises concerning the information environment?

Table 9 shows how DOD components identified past and planned actions to use or protect the information environment in their responses to our questionnaire.

Table 9: Categories of Actions DOD Components Have Undertaken or Plan to Undertake to Use or Protect the Information Environment

| Area | Undertaken between October 2018 and December 2021 | Area | Plan to undertake between December 2021 and September 2023 |
|-------------------|---|-------------------|--|
| Leadership | 24 | Policy | 23 |
| Training | 24 | Training | 23 |
| Policy | 23 | Plans | 21 |
| Materiel | 22 | Field exercises | 20 |
| Organization | 22 | Leadership | 20 |
| Plans | 21 | Materiel | 20 |
| Field exercises | 20 | Personnel | 20 |
| Command exercises | 19 | Organization | 19 |
| Facilities | 19 | Command exercises | 18 |
| Personnel | 19 | Doctrine | 15 |
| Doctrine | 17 | Facilities | 15 |
| Other | 6 | Other | 3 |

Source: GAO analysis of DOD components' responses to GAO's questionnaires. | GAO-22-104714



Agency Comments and Our Evaluation

We provided a draft of this report to the DOD for their review and comment. DOD concurred with our report and provided technical comments, which we addressed as appropriate. DOD's letter is included in appendix IV.

We are sending copies of this report to the appropriate congressional committees and Secretary of Defense. In addition, this report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or KirschbaumJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

In addition, Tommy Baril (Assistant Director), Neil Feldman (Analyst-in-Charge), Mallory Bryan, Evan Keir, and Ricardo Marquez made key contributions to this report. Tracy Barnes, Amie Lesser, Gabriel Nelson, Richard Powelson, Michael Silver, and Pamela Snedden also provided contributions.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Addressees

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

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Honorable Adam Schiff
Chairman
The Honorable Michael R. Turner
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Betty McCollum
Chair
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable Stephen F. Lynch
Chairman
Subcommittee on National Security
Committee on Oversight and Reform
House of Representatives

Evolution of Information as a Joint Function and Operations in the Information Environment

Information as a Joint Function

According to Joint Publication 3-0, *Joint Operations*, the information function encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision-making. It helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during military operations. The information function provides joint force commanders the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of military activities to achieve the commander's objectives and attain the end state.

All military activities produce information. Informational aspects are the features and details of military activities observers interpret and use to assign meaning and gain understanding. Those aspects affect the perceptions and attitudes that drive behavior and decision-making. The joint force commander leverages informational aspects of military activities to gain an advantage; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes.

The information function includes activities that facilitate the joint force commander's understanding of the role of information in the operational environment, facilitate the joint force commander's ability to leverage information to affect behavior, and support human and automated decision-making, as highlighted below.¹

- **Understanding information in the operational environment.** In conjunction with activities under the intelligence joint function, this activity facilitates the joint force commander's understanding of the pervasive nature of information in the operational environment, its impact on relevant actors, and its effect on military

operations. It includes determining relevant actor perceptions, attitudes, and decision-making processes and requires an appreciation of their culture, history, and narratives, as well as knowledge of the means, context, and established patterns of their communication.

- **Leveraging information to affect behavior.** Tasks aligned under this activity apply the joint force commander's understanding of the impact information has on perceptions, attitudes, and decision-making processes to affect the behaviors of relevant actors in ways favorable to joint force objectives. Related tasks include influencing relevant actors; informing domestic, international, and internal audiences; attacking and exploit information, information networks, and systems.
- **Supporting human and automated decision-making.** The management aspect of the information joint function includes activities that facilitate shared understanding across the joint force and that protect friendly information, information networks, and systems to ensure the availability of timely, accurate, and relevant information necessary for the joint force commander's decision-making. Related tasks include facilitating shared understanding; and, protecting friendly information, information networks, and systems.

Operations in the Information Environment

The National Defense Authorization Act for Fiscal Year 2014 directed the Secretary of Defense to develop and implement a strategy for developing and sustaining, through fiscal year 2020, information operations capabilities for future contingencies.² The Department of Defense addressed this mandate in October 2014 by issuing a report entitled *Developing and Sustaining Through Fiscal Year 2020 Military Information Operations Capabilities for Future Contingencies*.³ The report described how capabilities would be integrated, outlined joint force requirements, estimated the level of resources required through Fiscal Year 2020, and identified areas for future research.

¹DOD defines the operational environment as the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas of the air, land, maritime, and space domains; the information environment (which includes cyberspace); as well as the electromagnetic spectrum. Included within these are enemy, friendly, and neutral systems that are relevant to a specific joint operation. Joint Publication 3-0, *Joint Operations*, (Jan. 17, 2017, incorporating Change 1, October 22, 2018).

²Pub. L. No. 113-66, § 1096 (2013).

³DOD, *Developing and Sustaining through Fiscal Year 2020 Military Information Operations Capabilities for Future Contingencies* (October 2014).

In June 2016, the Secretary of Defense followed this report by issuing the *Department of Defense Strategy for Operations in the Information Environment*.⁴ Then Secretary of Defense Carter stated that, although the term information environment is relatively new, the concept of an “information battlefield” is not. He went on to say that the role of information, either provided or denied, is an important consideration in military planning and operations. Information is such a powerful tool, it is recognized as an element of U.S. national power and, as such, the department must be prepared to synchronize information programs, plans, messages, and products as part of a whole-of-government effort.

Since the issuance of the 2016 strategy, DOD has taken additional actions to evolve its conception of the information environment in policy and doctrine. In 2017, DOD updated its *Doctrine for the Armed Forces of the United States* to establish Information as the seventh joint function of the military, along with the joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.⁵ According to the *Doctrine*, the information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, action or inaction, and human and automated decision-making.

In 2018, DOD issued the *Joint Concept for Integrated Campaigning* which addresses DOD’s role in achieving goals outside of the traditional military sphere—such as competition below the threshold of armed conflict—and the *Joint Concept for Operating in the Information Environment* to institutionalize and operationalize the military’s approach to information operations.⁶ In 2018, DOD updated the discussion of the Information function in Joint Publication 3-0, *Joint Operations*.⁷ The publication states that all military activities produce information and that the joint force commander leverages informational aspects of military activities to gain an advantage and potentially affect the strategic outcome.

According to officials from the Joint Information Operations Warfare Center (JIOWC) with whom we spoke, DOD has drafted a new doctrine publication, Joint Publication 3-04, *Information in Joint Operations*, that will among other things, reframe the intellectual approach for how DOD considers operations in the information environment and revise the definitions of “information environment” and

related terms. According to DOD officials, Joint Publication 3-04 is expected to be issued later in 2022.

DOD Terms and Definitions

As noted above, the draft of Joint Publication 3-04, *Information in Joint Operations*, will also revise the definition of the information environment. While the current definition emphasizes the individuals, organizations, and systems that collect, process, disseminate, or act on information, the draft language under consideration emphasizes how intangible factors can affect how these actors derive meaning from, are impacted by, and act upon information. The draft language explains that the information environment is not distinct from any operational environment and that it is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decisions of the commander.

In addition to revising its definition of the information environment, the forthcoming Joint Publication 3-04 changes the terminology used to discuss operations in the information environment. For example, it removes terms such as information operations, information-related capability, and information superiority and replaces them with new definitions of information advantage and informational power. Figure 9 shows the evolution of some of this terminology.

⁴DOD, *Department of Defense Strategy for Operations in the Information Environment* (June 2016).

⁵Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Mar. 25, 2013, incorporating Change 1, July 12, 2017).

⁶Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning* (Mar. 16, 2018); *Joint Concept for Operating in the Information Environment (JCOIE)* (July 25, 2018).

⁷Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Jan. 17, 2017, incorporating Change 1, October 22, 2018).

Figure 9: Transition of Selected Information Environment-Related Terminology

| Current terms defined in Joint Publication 3-13 <i>Information Operations</i> or the 2018 <i>Joint Concept for Operating in the Information Environment</i> | New or revised terms to be defined in the draft Joint Publication 3-04 <i>Information in Joint Operations</i> |
|--|---|
| <p>Informational Power The ability to leverage information to shape the perceptions, attitudes, and other elements that drive desired behaviors and the course of events. This includes the ability to use information to affect the observations, perceptions, decisions, and behaviors of relevant actors; ability to protect and ensure the observations, perceptions, decisions, and behaviors of the Joint Force; and the ability to acquire, process, distribute, and employ data (information). This helps commanders and staffs incorporate the concept of the preeminent nature of information into the design of all operations to maximize military power.</p> | <p>→ Informational Power The ability to use information to support achievement of objectives and gain an informational advantage.</p> |
| <p>Information Superiority The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.</p> | <p>→ Information Advantage The operational advantage gained through the joint force's use of information for decision-making and its ability to leverage information to create effects on the Information Environment.</p> |
| <p>Information Operations Intelligence Integration The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment.</p> | <p>→ <i>Upon approval and publication of JP 3-04 Draft, this term will be removed from the DOD Dictionary.</i></p> |

Source: GAO analysis of Joint Publication 3-13 *Information Operations*, the *Joint Concept for Operating in the Information Environment* and the draft Joint Publication 3-04 *Information in Joint Operations*. | GAO-22-104714

Draft Joint Publication 3-04 also reframes the information environment *dimensions* into physical, informational, and human *aspects*. The Joint Publication explains that this updated model of the information environment does not separate these aspects into individual categories for individual analysis, but establishes a new approach that is a way of describing the different characteristics of objects, activities, or relevant actors; and the context in which they exist and are acted upon.

Together the three aspects provide the context needed to understand how individuals, groups, populations, and automated systems operate. The aspects collectively describe how a relevant actor receives information and describes the factors that affect the processing and interpretation of that information.

- The informational aspect reflects the way that individuals, information systems, and groups communicate and exchange information. This is the content, medium, format, and context of information transmittal and interpretation.
- The physical aspect refers to the material characteristics of the environment that may influence the ability to communicate. This can refer to a geographic or man-made structure in the environment or it can refer to other physical norms of communication among a given population (e.g., a preference for face-to-face communication rather than written or telephone communication).
- The human aspect refers to the interactions among and between people and how the environment shapes human behavior and decision-making. This aspect is based on the

linguistic, social, cultural, psychological, and physical elements of communication and impacts how the human mind applies meaning to the information it has received, i.e., how people think about information and make decisions based on this information.

The draft document states that the establishment of the Information joint function and subsequent revisions to joint publications constitute a significant doctrinal change. Specifically, the change from “joint information operations” to “operations in the information environment” presents a substantial force development challenge that requires the joint force to evaluate how to organize forces and staffs to deliberately plan and execute operations in the information environment.

Further, the draft document states that the military will apply informational power across the continuum of competition among state and non-state actors through leveraging informational aspects of traditional military operations as well as through operations in the information environment. Together, these can expand the commanders’ range of options to achieve their goals. Operations in the information environment calls for formations with the capabilities (i.e., the authorities and tools, as well as subject matter experts possessing in-depth skills, knowledge, and abilities to employ those tools) required to carry out actions that leverage information to affect behavior.

Upon approval of JP 3-04 Draft, these terms and their definitions will be removed from the DOD Dictionary

- **Information Operations.** The integrated employment during military operations of information-related capabilities in concert

with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

- **Information Operations Intelligence Integration.** The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment.
- **Information-related capability.** A tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials.
- **Information Superiority.** The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Upon approval of JP 3-04 Draft, these terms and their definitions will be added to the DOD Dictionary

- **Information Environment.** The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information.
- **Knowledge Management.** A discipline that integrates people and processes to create shared understanding, increased organizational performance, and improved decision-making.
- **Operations in the Information Environment.** Military actions involving the integrated employment of multiple information forces to affect drivers of behavior.
- **Relevant Actor.** Individual, group, population, or automated system whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action.
- **Target Audience.** An individual or group selected for influence.



Objectives, Scope, and Methodology

This report describes DOD's use and protection of the information environment through the following six key elements: (1) ubiquitous and malign information; (2) the information environment's effects on DOD's mission; (3) threat *actors* to the DOD Information Environment; (4) threat *actions* to the DOD Information Environment; (5) institutional challenges DOD faces in using the information environment; and, (6) emerging technologies that can enable or adversely affect DOD's missions in the information environment. The report also describes DOD actions taken from October 2018 through December 2021 and actions planned through September 2023 to use and protect the information environment.

To address these objectives, we administered a standardized questionnaire to a non-generalizable sample of 25 DOD organizations. We identified DOD organizations that perform under the authority, direction, and control of the Secretary of Defense; and have missions in the information environment by reviewing DOD guidance documents that define the roles and responsibilities of DOD components.¹ We transmitted the questionnaire to the Office of the Secretary of Defense, the Joint Staff (including the Joint Chiefs of Staff and the Joint Information Operations Warfare Center (JIOWC)), five military services,² 11 combatant commands, and 6 defense agencies and organizations.³

We requested that each DOD organization submit one questionnaire response back to us with the instruction that this questionnaire response should be informed by all subcomponents or lower-level offices with relevant subject matter expertise and vetted by the appropriate level of component senior leadership. We also provided to the DOD components a means for returning classified responses to the questionnaire.

The questionnaire contained ten sections with a total of twenty-two closed- and open-ended questions that aligned with the engagement objectives.⁴ A survey specialist helped to develop the questions, and another survey specialist provided independent

feedback on the questions. Nine GAO staff with expertise in military and/or technical concepts and terms also provided feedback on the questions. Additionally, officials from DOD's Joint Information Operations Warfare Center's Information Proponent Division provided feedback. We incorporated that feedback into the final version of the questionnaire.

To minimize errors that might occur from respondents interpreting our questions differently than we intended or that might introduce concerns related to classified material, we pretested our questionnaire with officials from five components, including one intelligence organization, one military service, one geographic combatant command, one functional combatant command, and one other DOD organization. During each pretest, all of which were conducted by phone, we tested the (1) clarity of the instructions and questions, (2) comprehensiveness of topics, questions, and response options; and, (3) ease of readability and navigation. We modified the questionnaire based on the feedback received. We noted any potential problems identified through the pretests and modified the questionnaire based on the feedback received. The optional classified version of the questionnaire was identical to the unclassified version with the exceptions that we asked responding organizations to provide an unclassified answer to all questions they provided a classified response for whenever possible and we included areas to provide classification markings for individual responses. Both versions were sent via email as Microsoft Word forms with fillable response fields. See appendix III for the unclassified version of the questionnaire and response options for questions summarized in this report.

We gathered responses to the questionnaire between August 19, 2021 and December 1, 2021. To maximize our response rate, we notified organizations that we would be sending a questionnaire, provided a separate set of instructions for how to complete the questionnaire, and sent reminder emails to encourage components to complete the questionnaire. We received responses

¹Department of Defense Directive 5100.01, *Functions of the Department of Defense and Its Major Components* (Dec. 21, 2010, incorporating Change 1, Sept. 17, 2020); Department of Defense Directive 3600.01, *Information Operations* (May 2, 2013, incorporating Change 1, May 4, 2017); and Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014).

²Although the U.S. Coast Guard is a military service, we did not include it in the scope of this engagement because it is a part of the Department of Homeland Security.

³The six defense agencies and organizations are the Defense Advanced Research Projects Agency (DARPA); Defense Digital Service (DDS); Defense Information Systems Agency (DISA); Defense Intelligence Agency (DIA); Defense Media Activity (DMA); and the National Security Agency (NSA).

⁴The closed-ended questions presented the respondent only with options for "Yes," "No," "Unknown," and, for some questions, "Not Applicable." Open-ended questions allowed the respondent to fill in narrative responses as they saw fit.

from all components, for a response rate of 100 percent, including classified responses from four components. After receiving responses, we communicated with some components to clarify unclear answers and adjusted the data to reflect the accurate and complete information.

For the unclassified questionnaires, responses to closed-ended questions were extracted from the unclassified Word forms and inserted into a delimited file that was imported into Excel, and that process was reviewed and verified for accuracy and completeness.⁵ We calculated the frequency of responses to our closed-ended questions and reviewed and summarized responses to the open-ended questions. One data analyst performed the quantitative analyses using Python and another data analyst reviewed the output and code to ensure their accuracy. For open-ended questions, engagement team analysts reviewed all responses and identified relevant examples to expand upon the results of the quantitative analysis conducted on the closed-ended responses.

For the classified responses from four DOD components, one analyst manually tabulated the unclassified answers to the closed-ended questions and another analyst independently verified the tabulations for accuracy and completeness. Those responses were combined with the quantitative analysis output from the unclassified responses and another analyst verified the entries and the final analysis. For open-ended questions, engagement team analysts reviewed all responses and identified relevant unclassified examples, as appropriate, to expand upon the results of the quantitative analysis conducted on the closed-ended responses.

Three DOD components provided more than one response (i.e., two lower-level offices provided separate responses rather than a single response on behalf of the entire component). In those cases, if any lower-level office answered “Yes” to a closed-ended question, we considered the overall answer for the component to be “Yes.” For two of the components that gave fully unclassified responses our data analyst performed this adjudication as part of the quantitative analysis described above. For the one component that provided unclassified responses from multiple lower-level offices as part of a classified package of questionnaire responses one analyst tabulated these answers manually and then another analyst independently verified the tabulations before they were included in the final analysis discussed above.

We developed and transmitted a separate questionnaire directed to the leadership of each of the 25 DOD organizations as the questionnaire. The leadership questionnaire requested responses from each recipient organization’s leadership (at the highest level possible) to the following three questions:

- What is [your organization’s] most important accomplishment in regard to the information environment since the elevation of “information” as a new and seventh joint function?
- As the component head of [your organization], what is your greatest concern for [your organization] regarding the information environment?
- What is the most important initiative [your organization] needs to take to utilize and protect the information environment in the next two years?

We received responses from all components, for a response rate of 100 percent. However, as those responses came from a variety of levels within the 25 DOD components, rather than the highest levels of leadership at each component, we only used the information received as context for our other analyses.

We interviewed officials from the Air Force, Defense Digital Service, Defense Intelligence Agency, Joint Information Operations Warfare Center, Marine Corps, Office of the Undersecretary of Defense for Policy, U.S. Southern Command, U.S. Space Command, and U.S. Strategic Command to obtain background information about the information environment or to test and refine our questionnaires.

Additionally, we interviewed subject matter experts knowledgeable in information environment matters. We selected individuals who (1) are currently serving or have served as decision-makers or principals in governmental, academic, business, or professional organizations outside of DOD or formerly as DOD officials; (2) are recognized as experts in governmental, academic, business, or professional communities based on their affiliation, publications, reputation in the national security community, or testimony before Congress; (3) have been responsible for issuing official government guidance, regulations, or publications recognized as principal resources for research and analysis. On this basis, we interviewed the following nine subject matter experts:

⁵Four components returned PDF copies of their unclassified Word responses rather than the Word form itself. One analyst manually entered the responses into a Word form and another analyst verified the accuracy and completeness of the data entry. Responses were then extracted from that Word form along with all the others.

- Lieutenant General (retired) Edward Cardon (Commanding General, U.S. Army Cyber Command from 2013 to 2016)
- Mr. Glenn Gerstell (Center for Strategic and International Studies)
- Ms. Nina Jankowicz (Wilson Center)
- Dr. Herb Lin (Stanford University)
- Ms. Samantha Ravich (Cyberspace Solarium Commission)
- Mr. Michael Schwille (RAND)
- Dr. Peter Singer (New America)
- Ms. Catherine A. Theohary (Congressional Research Service)
- Mr. Matt Venhaus (University of Maryland, Applied Research Laboratory for Intelligence and Security)

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 also interviewed board members from the Information Professionals Association: Mr. Austin Branch, Dr. Barton Brown, Mr. Kevin Gates, Dr. Paul Leiber, Ms. Paula Trimble, Mr. Matt Venhaus, Mr. Rand Waltzman, and Mr. Mike Williams.

Further, we reviewed 35 strategy, policy, doctrine, and guidance documents from DOD and other federal government agencies to inform our understanding of DOD's prior work and current approach to the information environment. These were the most recent publications available, having been published from 2015-2022. We also reviewed approximately 180 white papers, studies, and news articles related to the information environment to provide a background understanding of how private industry, academic institutions, and the news media are describing and communicating this topic.⁶

We developed questions for oversight for each of the information environment profile sheets. The questions were developed based on our discussions with DOD officials and external subject matter experts, analysis of DOD's responses to our component and leadership questionnaires, and a review of recent GAO work relevant to the information environment. During the conduct of this review, engagement team analysts also continuously identified topics and collaborated on the development of questions.

We conducted this performance audit from January 2021 to July 2022 in accordance with generally

⁶Due to the nebulous nature of the information environment and its evolving definition and understanding, these documents were reviewed at the summary level for relevance to the information environment as defined by Joint Publication 3-13, which served as the initial operational definition used for our review. Sixty-nine were selected as relevant to our operational definition and were used to inform our understanding of the information environment and development of the topics in this report. These documents were published between 2011 and 2021.



Questionnaire Administered to DOD Components

To address our objectives, we administered a standardized questionnaire to a non-generalizable sample of 25 DOD organizations. The questionnaire contained 10 sections with a total of 22 closed- and open-ended questions that aligned with the engagement objectives. A description of our process

for developing and administering the questionnaire, and analyzing the responses can be found in appendix II. The verbatim wording of key survey questions whose results are described in this report is below:

SECTION III. INFORMATION ENVIRONMENT’S RELATIONSHIP TO YOUR ORGANIZATION’S MISSION

3. In the following table, please tell us whether the Information Environment impacts [ORG]’s function/mission and which 5 functions/missions are most impacted. Please select an answer about impact for each row that names a function/mission. Additionally, please feel free to include any other function/mission we have not listed in the spaces provided that is impacted by the Information Environment. If you aren’t sure whether the Information Environment impacts [ORG]’s function/mission, please select “Unk (unknown). If any of the listed functions/missions are not part of [ORG]’s roles, please select “N/A” (Not Applicable). After answering the impact questions, please select the five functions/missions that are most impacted by the Information Environment by selecting up to five boxes in the last column.

| Function/Mission | Impact? <i>Please check one box per row.</i> | Top 5? |
|---------------------|---|--------|
| Business operations | Yes No Unk N/A | |

The DOD components were provided with the following list of response options for question #3:

- Business operations
- Command-and-control decision-making
- Communications
- Conduct military operations
- Coordination with allies and partners
- Day-to-day decision-making
- Intelligence and counterintelligence activities
- DOD coordination with other agencies
- Conduct law enforcement activities
- Maintain organization cohesion, morale, or discipline
- Hire, train, or retain personnel
- Acquire and sustain equipment
- Provide logistical support
- Oversight of lower echelon organizations
- Policy, plans, or doctrine development
- Research and Development
- Security (e.g., OPSEC and INFOSEC)
- Other [A text box was provided]

4. For the functions/missions that you answered “Yes” to in the Question 3 table on the last few pages and above, please select three that are most important to your organization and provide one example of the impact of the information environment on that function/mission. *The boxes will expand as you type.*

Example (Please indicate the function/mission within the example): [Three text boxes were provided]

SECTION IV. THREATS ASSOCIATED WITH THE INFORMATION ENVIRONMENT

Joint Publication 3-0, *Joint Operations*, provides the following definitions for the informational, physical, and human aspects of the Information Environment (IE):

“Informational aspects reflect the way individuals, information systems, and groups communicate and exchange information.”

For example, threats to the informational aspects of the IE could include, but are not limited to, actions taken against data, information, software, applications, and internet sites (e.g. data and information exfiltration, manipulation, and/or destruction; presenting misinformation and/or disinformation; signature management, collection of information about operations and DOD persons; using bots and/or fake personas; etc.).

[A footnote explained that “For this request for information, “DOD persons” refers to service members, employees, contractors, and DOD family members (i.e., dependents).”]

“Physical aspects are the material characteristics of the environment that create constraints on and freedoms for the people and information systems that operate in it.”

For example, threats to the physical aspects of the IE could include, but are not limited to, actions taken against physical, cyberspace, space, and EMS systems and capabilities (e.g. exploit information and communications technology supply chain, jamming electronic capabilities, etc.).

“Human aspects frame why relevant actors perceive a situation in a particular way.”

For example, threats to the human aspects of the IE could include, but are not limited to, actions taken to influence decision-making (e.g., target DOD persons with misinformation and/or disinformation in an effort to have them take specific actions, decrease unit morale, question decisions of leadership, etc.).

5. In the following table, please tell us whether your organization considers each of the listed actors to be a threat to [ORG] in the Information Environment, and which five actors [ORG] considers to be its most important. Please select an answer for each row that provides a named actor. Additionally, please feel free to include any other threat actors we have not listed in the spaces provided. If you aren't sure whether an actor is a threat to [ORG] in the Information Environment, please select "Unk" (unknown). For the actors that you answered "yes" as a threat to [ORG] in the Information Environment, please select the five actors that [ORG] considers to be its most important by selecting up to five boxes in the last column.

| Actor | Threat? <i>Please check one box per row.</i> | Top 5? |
|-------|---|--------|
| China | Yes No Unk | |

The DOD components were provided with the following list of response options for question #5:

- China
- Russia
- Iran
- North Korea
- Foreign terrorists (e.g., ISIS, Al-Shabaab, Boko Haram, etc.)
- U.S. Domestic violent extremists (Please see footnote 2)
- Transnational organized criminal organizations (Please see footnote 3)
- Insider threats (intentional and/or unintentional)
- Individuals/Lone-wolf actors (excluding Insider Threat)
- Allies or partners
- U.S. or foreign corporations
- Special interest groups
- Other [A text box was provided]

[Footnote 2 stated: "According to DHS, FBI, and ODNI definitions and terminology, domestic violent extremism (DVE) encompasses an individual or group of individuals who are based and operate primarily in the United States without direction or inspiration from a foreign terrorist group or other foreign power and who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. Such acts are dangerous to human life and are a violation of the criminal laws of the United States or of any State. Such acts appear to be intended to intimidate or coerce a civilian population; influence the policy of government by intimidation or coercion; or, affect the conduct of a government by mass destruction, assassination or kidnapping; and, occur primarily within the territorial jurisdiction of the United States. This assessment does not evaluate the actions of individuals engaged solely in activities protected by the First Amendment or other rights secured by the Constitution of the United States."

Footnote 3 stated: "According to FBI terminology, transnational organized crime are self-perpetuating associations of individuals who operate, wholly or in part, by illegal means and irrespective of geography."

6. Please provide examples of how three different threat actors that you answered “Yes” to in the Question 5 table on the last few pages pose a threat to [ORG] in the Information Environment. The examples should reflect threats relevant to [ORG]’s mission, not just relevant to the entire Department of Defense. Please provide an example of a threat in the informational aspect of the IE, an example of a threat in the physical aspect of the IE, and an example of a threat in the human aspect of the IE. Please also provide at least one example that is NOT from a nation-state unless you have not selected “Yes” for any non-nation-state.

The boxes will expand as you type.

Informational Aspect example (Please indicate the actor within the example): [A text box was provided]

Physical Aspect example (Please indicate the actor within the example): [A text box was provided]

Human Aspect example (Please indicate the actor within the example): [A text box was provided]

7. In the following table, please tell us whether your organization considers each of the listed actions to be a threat to [ORG] in the Information Environment, and which five actions [ORG] considers to be its most important. Please select an answer for each row that provides a named action. Additionally, please feel free to include any other actions we have not listed in the spaces provided. If your organization is not aware of whether a particular action is a threat to your organization, please select “Unk” (unknown). For the actions that you answered “yes” as a threat to [ORG] in the Information Environment, please select the five actions that [ORG] considers to be its most important by selecting up to five boxes in the last column.

| Action | Threat? <i>Please check one box per row.</i> | Top 5? |
|--|---|--------|
| Physical attacks against [ORG] information systems | Yes No Unk | |

The DOD components were provided with the following list of response options for question #7:

- Physical attacks against [ORG] information systems
- Malicious cyber activity against [ORG] information systems
- Actions to implant, modify, destroy, or extract data within [ORG] information systems
- Collection of information or intelligence to understand [ORG]’s mission, operations, or personnel
- Physical attacks against [ORG] electromagnetic spectrum (EMS) capabilities
- Malicious use of the EMS to degrade or damage capabilities
- Malicious use of EMS to harm [ORG] personnel (including service members and civilian personnel), contractors, or family members
- Physical attacks against [ORG] personnel (including service members and civilian personnel), contractors, or family members
- Target or try to influence policy making or planning efforts
- Target or try to influence commander’s/leader’s command-and-control decision-making process
- Target or try to influence service members’ or employees’ morale or decision-making
- Other [A text box was provided]

8. Please provide examples of how three different threat actions that you answered “Yes” to in the Question 7 table on the last few pages pose a threat to [ORG] in the Information Environment. The examples should reflect threats relevant to [ORG]’s mission, not just relevant to the entire Department of Defense. Please provide an example of a threat in the informational aspect of the IE, an example of a threat in the physical aspect of the IE, and an example of a threat in the human aspect of the IE. *The boxes will expand as you type.*
- Informational Aspect example (Please indicate the action within the example): [A text box was provided]
- Physical Aspect example (Please indicate the action within the example): [A text box was provided]
- Human Aspect example (Please indicate the action within the example): [A text box was provided]

SECTION V. PAST AND ONGOING ACTIONS TO UTILIZE OR PROTECT THE INFORMATION ENVIRONMENT

Joint Publication 3-0 *Joint Operations* provides the following definitions for the informational, physical, and human aspects of the Information Environment:

“Informational aspects reflect the way individuals, information systems, and groups communicate and exchange information.”

“Physical aspects are the material characteristics of the environment that create constraints on and freedoms for the people and information systems that operate in it.”

“Human aspects frame why relevant actors perceive a situation in a particular way.”

9. In the following table, please tell us whether your organization has undertaken actions to utilize or protect the Information Environment from October 2018 (when information was identified as a joint function in joint doctrine) to the present. Please select an answer for each row that provides a named action. Additionally, please feel free to include any other actions we have not listed in the spaces provided. If you aren't sure whether your organization has undertaken actions in an area, please select "Unk" (unknown). If your organization does not have responsibility for an action listed, please select "N/A" (Not Applicable).

| Action | Action Taken or Ongoing? <i>Please check one box per row.</i> | Top 5? |
|--|--|--------|
| Policy, guidance, regulations, or instructions (e.g., issue, update, etc.) | Yes No Unk N/A | |

The DOD components were provided with the following list of response options for question #9:

- Policy, guidance, regulations, or instructions (e.g., issue, update, etc.)
- Doctrine (e.g., issue, update, etc.)
- Plans (e.g., develop, update, etc.)
- Organization (e.g., realign, establish new office or position, etc.)
- Training (e.g., develop, modify, offer, etc.)
- Materiel (e.g., obtain, modernize, etc.)
- Leadership (e.g., demonstrate, emphasize priority, etc.)
- Personnel (e.g., dedicate personnel, establish new career path, etc.)
- Facilities (e.g., modify, obtain, etc.)
- Field Exercises (e.g., conduct, participate in another component's, etc.)
- Command/Table-Top Exercises (e.g., conduct, participate in another component's, etc.)
- Other [A text box was provided]

10. For three of the actions that you answered “Yes” to in the Question 9 table on the last few pages, please discuss actions taken, with one example for each of the aspects (informational, physical, and human) of the IE, and describe the benefits received to [ORG] from each action. The boxes will expand as you type.

Informational Aspect example (Please indicate the action within the example): [A text box was provided]

Physical Aspect example (Please indicate the action within the example): [A text box was provided]

Human Aspect example (Please indicate the action within the example): [A text box was provided]

11. If [ORG] has conducted operations to utilize or protect the Information Environment, please provide one example in any of the three aspects from October 2018 (when information was identified as a joint function in joint doctrine) to the present and describe how [ORG] benefited from this example. The box will expand as you type. [A text box was provided]

SECTION VI. PLANNED ACTIONS TO UTILIZE OR PROTECT THE INFORMATION ENVIRONMENT

[The definitions of informational, physical, and human aspects of the Information Environment from Joint Publication 3-0, *Joint Operations* were repeated here for the respondents' reference.]

12. In the following table, please tell us whether your organization is planning to undertake new actions to utilize or protect the Information Environment in the listed areas below from the present to the end of September 2023—i.e., over the next two fiscal years. Planned actions include the continuation of those past actions from the response to the previous questions. Please select an answer for each row that provides a named action. Additionally, please feel free to include any other actions we have not listed in the spaces provided. If you aren't sure whether your organization is planning to undertake new actions in an area, please select “Unk” (unknown). If your organization does not have responsibility for a type of action listed, please select “N/A” (Not Applicable).

| Action | Action Planned? <i>Please check one box per row.</i> |
|--|---|
| Policy, guidance, regulations, or instructions (e.g., issue, update, etc.) | Yes No Unk N/A |

The DOD components were provided with the following list of response options for question #12:

- Policy, guidance, regulations, or instructions (e.g., issuing, updating, etc.)
- Doctrine (e.g., issuing, updating, etc.)
- Plans (e.g., developing, updating, etc.)
- Organization (e.g., realigning, establishing new office or position, etc.)
- Training (e.g., developing, modifying, offering, etc.)
- Materiel (e.g., obtaining, modernizing, etc.)
- Leadership (e.g., demonstrating, emphasizing priority, etc.)
- Personnel (e.g., dedicating personnel, establishing new career path, etc.)
- Facilities (e.g., modifying, obtaining, etc.)
- Field Exercises (e.g., conducting, participating in another component's, etc.)
- Command/Table-Top Exercises (e.g., conducting, participating in another component's, etc.)
- Other [A text box was provided]

13. For three of the actions that you answered “Yes” to in the Question 12 table on the last few pages, please discuss three planned actions, with one example for each of the aspects (informational, physical, and human) of the IE. Describe the benefits expected to [ORG] from each action, and identify the timeframe for their implementation. *The boxes will expand as you type.*

Informational Aspect example (Please indicate the action within the example): [A text box was provided]

Physical Aspect example (Please indicate the action within the example): [A text box was provided]

Human Aspect example (Please indicate the action within the example): [A text box was provided]

SECTION VII. INSTITUTIONAL CHALLENGES ASSOCIATED WITH THE INFORMATION ENVIRONMENT

[The definitions of informational, physical, and human aspects of the Information Environment from Joint Publication 3-0 *Joint Operations* were repeated here for the respondents' reference.]

14. In the following table, please tell us whether your organization considers each of the listed issue areas below to be a challenge related to the Information Environment and which five challenges [ORG] considers to be its most important. The responses should reflect the challenges specific to [ORG], not challenges to the entire Department of Defense. Please select an answer for each row that provides a named issue. Additionally, please feel free to include any other institutional challenges we have not listed in the spaces provided. If you aren't sure whether your organization considers an issue a challenge, please select "Unk" (unknown). For the issue areas that you answered "yes" as a challenge to [ORG] in the Information Environment, please select the five that [ORG] considers to be its most important by selecting up to five boxes in the last column.

| Issue | Action Taken or Ongoing? <i>Please check one box per row.</i> | Top 5? |
|---|--|--------|
| Policy, guidance, regulations, or instructions (e.g., inadequate, insufficient, outdated, etc.) | Yes No Unk | |

The DOD components were provided with the following list of response options for question #14:

- Policy, guidance, regulations, or instructions (e.g., inadequate, insufficient, outdated, etc.)
- Doctrine (e.g., inadequate, insufficient, outdated, etc.)
- Plans (e.g., inadequate, insufficient, outdated, etc.)
- Organization (e.g., structure/alignment is inadequate, insufficient, outdated, etc.)
- Training (e.g., inadequate, insufficient, outdated, etc.)
- Materiel (e.g., inadequate, insufficient, outdated, etc.)
- Leadership (e.g., preparation for and understanding of IE-related challenges and issues, etc.)
- Personnel (e.g., inadequate, insufficient, etc.)
- Facilities (e.g., inadequate, insufficient, outdated, etc.)
- Interagency Coordination (e.g., structure/alignment is inadequate, insufficient, etc.)
- Coordination with Allies and Partners (e.g., structure/alignment is inadequate, insufficient, etc.)
- Data and Information (e.g., inadequate, insufficient, outdated, etc.)
- Information Technology hardware, software, tools, etc. (e.g., inadequate, insufficient, outdated, etc.)
- Funding (e.g., inadequate, insufficient, misprioritized, etc.)
- Other [A text box was provided]

15. For three of the items that you answered “Yes” to in the Question 14 table on the last few pages, please discuss one example of institutional challenges to [ORG] for each of the aspects of the IE—informational, physical, and human. The responses should reflect the challenges specific to [ORG], not challenges to the entire Department of Defense. *The boxes will expand as you type.*

Informational Aspect example (Please indicate the issue within the example): [A text box was provided]

Physical Aspect example (Please indicate the issue within the example): [A text box was provided]

Human Aspect example (Please indicate the issue within the example): [A text box was provided]

SECTION VIII. EMERGING TECHNOLOGIES

This section is intended to determine what, if any, emerging technologies your organization considers potential threats or opportunities associated with the Information Environment.

As technologies emerge, they will accelerate change and introduce both threats and opportunities.

Examples of emerging technologies include, but are not limited to, artificial intelligence, quantum computing, blockchain, and the Internet of Things (IoT).

Please provide answers about threats and opportunities in each of the three aspects of the Information Environment below.

Informational Aspect:

“Informational aspects reflect the way individuals, information systems, and groups communicate and exchange information.” (Source: Joint Publication 3-0 Joint Operations)

16. What emerging technology(s), if any, has [ORG] identified as a threat to [ORG] in the informational aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]

17. What emerging technology(s), if any, has [ORG] identified as an opportunity for [ORG] in the informational aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]

Physical Aspect:

“Physical aspects are the material characteristics of the environment that create constraints on and freedoms for the people and information systems that operate in it.”

18. What emerging technology(s), if any, has [ORG] identified as a threat to [ORG] in the physical aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]

19. What emerging technology(s), if any, has [ORG] identified as an opportunity for [ORG] in the physical aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]

Human Aspect:

“Human aspects frame why relevant actors perceive a situation in a particular way.”

20. What emerging technology(s), if any, has [ORG] identified as a threat to [ORG] in the human aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]

21. What emerging technology(s), if any, has [ORG] identified as an opportunity for [ORG] in the human aspect of the IE? Please provide at least one example and briefly explain the rationale for this determination. *The box will expand as you type.* [A text box was provided]



SPECIAL OPERATIONS
LOW INTENSITY CONFLICT

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2500 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2500

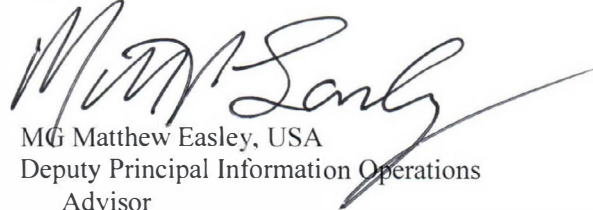
Mr. Joseph Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Kirschbaum,

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-22-104714, INFORMATION ENVIRONMENT: Opportunities and Threats to DOD's National Security Mission, dated September 2022.

The DoD concurs with the draft report with no substantive comments. Administrative (technical) comments will be provided separately. My point of contact is Mr. John Zabel. He may be reached at john.e.zabel.civ@mail.mil or 571-372-3347.

Sincerely,



MG Matthew Easley, USA
Deputy Principal Information Operations
Advisor

Related GAO Products

Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance. [GAO-22-105834](#). Washington, D.C.: March 30, 2022.

Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems. [GAO-22-104765](#). Washington, D.C.: February 17, 2022.

Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents. [GAO-22-104746](#). Washington, D.C.: January 13, 2022.

Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework. [GAO-22-104679](#). Washington, D.C.: December 8, 2021.

Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. [GAO-21-519SP](#). Washington, D.C.: June 30, 2021.

Technology Assessment: Defense Navigation Capabilities. [GAO-21-320SP](#). Washington, D.C.: May 10, 2021.

Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities. [GAO-21-525T](#). Washington, D.C.: April 30, 2021.

High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges. [GAO-21-288](#). Washington, D.C.: March 24, 2021.

Electromagnetic Spectrum Operations: DOD Needs to Take Action to Help Ensure Superiority. [GAO-21-440T](#). Washington, D.C.: March 19, 2021.

National Security: Actions Needed to Address 5G Telecommunications Risks. [GAO-21-256SU](#). Washington, D.C.: March 5, 2021.

High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. [GAO-21-119SP](#). Washington, D.C.: March 2, 2021.

Defense Transportation: DOD Can Better Leverage Existing Contested Mobility Studies and Improve Training. [GAO-21-125](#). Washington, D.C.: February 26, 2021.

Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority. [GAO-21-64](#). Washington, D.C.: December 10, 2020.

Cyberspace Operations: DOD Has Authorities and Organizations in Place, but Policies, Processes, and Reporting Could Be Improved. [GAO-20-13C](#). Washington, D.C.: September 28, 2020.

Internet of Things: Information on Use by Federal Agencies. [GAO-20-577](#). Washington, D.C.: August 13, 2020.

Science & Tech Spotlight: Quantum Technologies. [GAO-20-527SP](#). Washington, D.C.: May 28, 2020.

Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene. [GAO-20-241](#). Washington, D.C.: April 13, 2020.

Information Operations: DOD Should Improve Leadership and Integration Efforts. [GAO-20-51SU](#). Washington, D.C.: October 18, 2019.

Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations. [GAO-19-570](#). Washington, D.C.: August 15, 2019.

Ground Combat Forces: The Marine Corps Should Take Actions to Track Training Funds and Link Them to Readiness. [GAO-19-233](#). Washington, D.C.: April 8, 2019.

DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. [GAO-19-362](#). Washington, D.C.: March 6, 2019.

National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies. [GAO-19-204SP](#). Washington, D.C.: December 13, 2018.

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

Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems. [GAO-15-544](#). Washington, D.C.: June 2, 2015.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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 [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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

