Highlights of GAO-22-104714, a report to congressional addressees

Information Environment

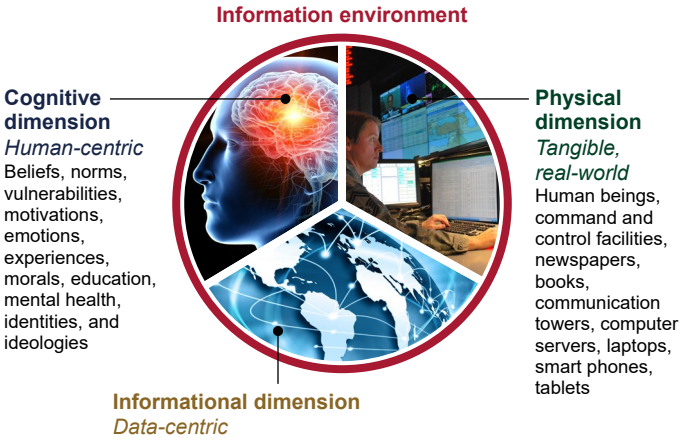
Opportunities and Threats to DOD's National Security Mission

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.

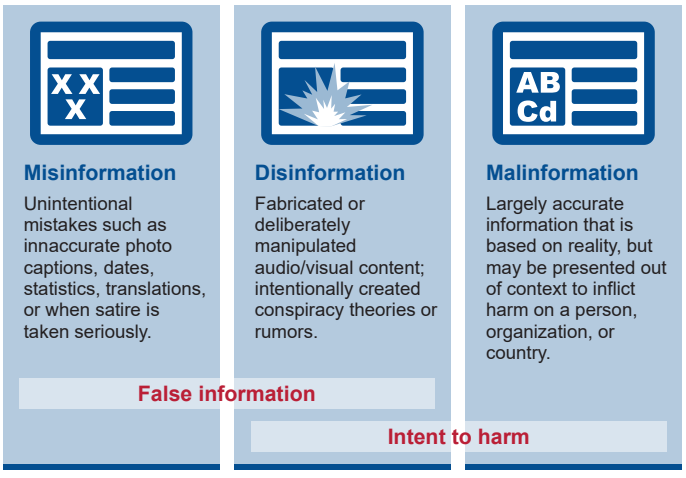
To prepare this report, among other things, GAO administered questionnaires to 25 DOD organizations involved in the information environment. GAO staff also interviewed officials and subject matter experts; reviewed 35 documents on strategy, policy, doctrine, and other guidance from DOD and other federal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

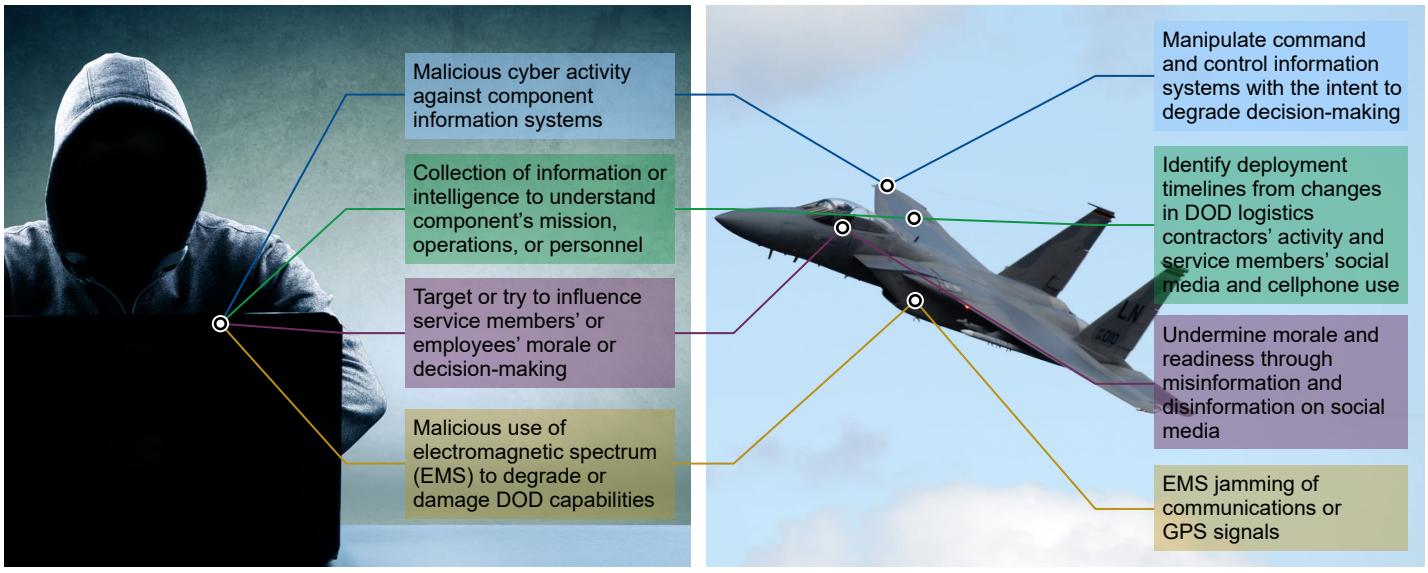
Institutional Challenges. National and DOD strategies and documents identify a number of institutional challenges that DOD must address. The challenges include a lack of leadership emphasis, lack of resources, the implications of new technologies, and dated processes. DOD components identified personnel, 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