Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 12, 2019

Defense Primer: Emerging Technologies

Senior U.S. defense and intelligence officials have identified a number of emerging technologies that could have a disruptive impact on U.S. national security in the years to come. These technologies include

- artificial intelligence,
- lethal autonomous weapons,
- hypersonic weapons,
- directed-energy weapons,
- biotechnology, and
- quantum technology.

As these technologies continue to mature, they could hold significant implications for congressional oversight, U.S. defense authorizations and appropriations, military concepts of operations, and the future of war.

Artificial Intelligence

Artificial intelligence (AI) refers to a computer system capable of human-level cognition. AI is currently being incorporated into a number of military applications, including intelligence, surveillance, and reconnaissance; logistics; defensive cyber operations; command and control; and semi-autonomous and autonomous vehicles. As it develops, AI could enable new concepts of operations, such as swarming (i.e., cooperative behavior in which uninhabited vehicles autonomously coordinate to achieve a task), that could present both challenges and opportunities for the U.S. military.

Recent news reports and analyses have highlighted the role of AI in enabling increasingly realistic photo, audio, and video digital forgeries, popularly known as "deep fakes." Adversaries could potentially deploy this AI capability as part of their information operations in a "gray zone" conflict. Deep fake technology could be used against the United States and its allies to generate false news reports, influence public discourse, erode public trust, and attempt to blackmail diplomats. Some have suggested that AI could be used to create full digital "patterns-of-life," in which an individual's digital footprint is mapped against other personal information, such as spending habits and job history, to create comprehensive behavioral profiles of servicemembers, suspected intelligence officers, government officials, and private citizens. Similar to deep fakes, this information could, in turn, be used for targeted influence operations or blackmail.

To coordinate defense-wide AI efforts, the Pentagon established the Joint Artificial Intelligence Center (JAIC, pronounced "jake") in June 2018 under the Department of Defense's (DOD's) Chief Information Officer. In addition, the FY2019 National Defense Authorization Act (P.L. 115-232, §1051) established a National Security Commission on Artificial Intelligence to assess U.S. competitiveness in AI and offer recommendations to Congress.

Lethal Autonomous Weapons

Lethal Autonomous Weapon Systems (LAWS) are a class of weapon systems capable of independently identifying a target and employing an onboard weapon system to engage and destroy the target with no human interaction. LAWS require computer algorithms and sensor suites to classify an object as hostile, make an engagement decision, and guide a weapon to the target. This capability would enable the system to operate in communications-degraded or -denied environments where traditional systems may not be able to operate.

LAWS do not yet exist, and some senior military and defense leaders have expressed concerns about the ethics of ever fielding such systems. For example, in 2017 testimony before the Senate Armed Services Committee, Vice Chairman of the Joint Chiefs of Staff General Paul Selva stated, "I do not think it is reasonable for us to put robots in charge of whether or not we take a human life." Currently, there are no domestic or international legal prohibitions on the development of LAWS; however, an international group of government experts has begun to discuss the issue. Approximately 25 countries have called for a preemptive ban on the systems due to ethical considerations, while others have called for formal regulation. DOD Directive 3000.09 establishes department guidelines for the development and fielding of LAWS to ensure that they comply with "the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement."

Hypersonic Weapons

Hypersonic weapons—which fly at speeds of at least Mach 5—do not yet exist, but they are in development in a number of countries. There are two categories of hypersonic weapons:

- **Hypersonic glide vehicles (HGV)** are launched from a rocket before gliding to a target.
- **Hypersonic cruise missiles (HCM)** are powered by high-speed engines throughout the duration of their flight.

In contrast to ballistic missiles, hypersonic weapons do not follow a ballistic trajectory and can maneuver en route to their destination, making defense against them difficult. Currently, no such defense against hypersonic weapons exists, and experts disagree on the affordability, technological feasibility, and utility of hypersonic missile defense options. These options could include interceptor

missiles, hypervelocity projectiles, laser guns, and electronic attack systems.

According to open-source reporting, China and Russia conducted successful hypersonic weapons tests in 2018 and are expected to have an operational HGV capability as early as 2020. The United States anticipates achieving an HGV capability around 2022. Although HCM technology is less mature than HGV technology, reports suggest that it could be fielded by Russia in 2022. Other countries—including France, Australia, India, and Germany—also have research programs in hypersonic weapons.

Directed-Energy Weapons

DOD defines directed-energy (DE) weapons as those using concentrated electromagnetic energy, rather than kinetic energy, to "incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel." DE weapons—often colloquially referred to as "lasers"—could be used by ground forces in counter rocket, artillery, and mortar (C-RAM) or short-range air defense (SHORAD) missions. They could offer low costs per shot and nearly limitless magazines that, in contrast to existing conventional systems, could enable an efficient and effective means of defending against missile salvos and swarms of uninhabited vehicles. Theoretically, DE weapons could also provide options for boost-phase missile defense, given their speed-of-light travel time; however, as in the case of hypersonic missile defense, experts disagree on the affordability, technological feasibility, and utility of this application.

High-powered microwave (HPM) weapons, a subset of DE weapons, could be used as a nonkinetic means of disabling electronics, communications systems, and improvised explosive devices in the event of a conflict. In addition, the U.S. military has explored using HPM in a nonlethal "heat ray" system for crowd control; however, the system was recalled—likely due to ethical and operational considerations.

Biotechnology

Biotechnology leverages life sciences for technological applications. A number of developments in biotechnology hold potential implications for national security. As a 2018 Government Accountability Office (GAO) report notes, the Departments of Defense, State (State), and Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI), all assess that biotechnologies, such as the low-cost gene-editing tool CRISPR-Cas9, have the potential to "alter genes or create DNA to modify plants, animals, and humans. Such biotechnologies could be used to enhance [or degrade] the performance of military personnel. The proliferation of synthetic biology—used to create genetic code that does not exist in nature—may increase the number of actors that can create chemical and biological weapons." U.S. adversaries may be less restrained in both researching and applying biotechnology, particularly as it relates to human performance modification and biological weapons.

Quantum Technology

Quantum technology**,** which employs the principles of quantum physics, has not yet reached maturity; however, it holds significant implications for the future of encryption and stealth technologies. GAO reports that DOD, State, DHS, and the ODNI have assessed that "quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt. Quantum computing may allow adversaries to decrypt [unclassified, classified, or sensitive] information, which could enable them to target U.S. personnel and military operations."

Quantum technology could have other military applications, such as quantum radar systems hypothesized to be capable of identifying the performance characteristics (e.g., radar cross-section, speed) of objects with a greater level of accuracy than conventional radar systems. This would significantly ease the tracking and targeting of U.S. low-observable, or stealth, aircraft such as the F-22, F-35, and B-2. Similarly, advances in quantum sensing could theoretically enable significant improvements in submarine detection, rendering the oceans "transparent." This could, in turn, hold implications for the survivability of the U.S. sea-based nuclear deterrent.

CRS Products

CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler

CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary

CRS Report R44466, *Lethal Autonomous Weapon Systems: Issues for Congress*, by Nathan J. Lucas

CRS Report R45098, *U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress*, by Andrew Feickert

CRS Report R44175, *Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress*, by Ronald O'Rourke

CRS Report R44824, *Advanced Gene Editing: CRISPR-Cas9*, by Marcy E. Gallo et al.

CRS Report R45409, *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations*, by Patricia Moloney Figliola

Other Resources

Department of Defense Directive 3000.09, "Autonomy in Weapon Systems," May 8, 2017, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

Government Accountability Office, *National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies*, December 2018, https://www.gao.gov/assets/700/695981.pdf.

Daniel R. Coats, "Statement for the Record: World Wide Threat Assessment of the U.S. Intelligence Community," January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf.

Kelley M. Sayler, Analyst in Advanced Technology and Global Security

Disclaimer