Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 13, 2019

Convergence of Cyberspace Operations and Electronic Warfare

Over the past two decades, cyberspace operations have become an important element in military operations. Electronic warfare (EW) has been a component of military operations since the advent of the radio at the beginning of the 20th century. These two types of operations are becoming somewhat analogous as technical capabilities converge, yet historical divides between EW and cyber operations remain in Department of Defense (DOD) organization and doctrine.

Both cyberspace operations and EW are efforts to dominate aspects of the electromagnetic spectrum (EMS) that transmit packets of information. As such, EW and cyberspace operations have traditionally been used as part of a broader information operations (IO) campaign, and previously existed in joint doctrine as two of the five pillars of IO (along with psychological operations, military deception, and operations security). These capabilities are increasingly being used in support of operations in the information environment (IE)—the aggregate of social, cultural, cognitive, technical and physical attributes that ultimately affect action. Current and evolving DOD doctrine refers to EMS operations and cyberspace operations as separate but related to operations in the IE.

Cyberspace Operations (CO)

Cyberspace operations are defined by DOD as the military, intelligence, and ordinary business operations of the DOD in and through cyberspace. Military cyberspace operations use cyberspace capabilities to create effects that support missions in both physical domains and cyberspace.

DOD categorizes cyberspace operations as follows:

- **Offensive cyberspace operations**, intended to project power by the application of force in and through cyberspace. These operations are authorized like operations in the physical domains.
- **Defensive cyberspace operations**, intended to defend DOD or other friendly cyberspace. Defense operations are both active and passive conducted inside and outside of DOD information networks (DODIN).
- **DODIN operations**, to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks across the entire DODIN.

Electronic Warfare (EW)

Since the introduction of two-way radios, militaries have become highly dependent on the EMS. This reliance has expanded over the past century to include nearly every weapon system. Applications include

- radio frequencies to communicate with friendly forces;
- microwaves for tactical data-links, radars, and satellite communications;
- infrared for intelligence and to target enemies; and
- lasers to communicate, transmit data, and potentially destroy a target.

Modern militaries rely on communications equipment that uses broad portions of EMS to conduct military operations. This allows forces to talk, transmit data, provide navigation and timing information, and to command and control forces all over the world. They also rely on the EMS to determine where adversaries are and what they are doing, where friendly forces are, and what effects weapons achieve. Because of this dependency, modern militaries attempt to dominate EMS through electronic warfare.

From the perspective of military operations, there are three broad divisions of electronic warfare:

- **Electronic protection** involves actions to protect access to EMS for friendly military assets.
- **Electronic attack** uses electromagnetic energy to degrade or deny an enemy's use of EMS.
- **EW support** identifies and catalogues emissions of friendly or enemy forces either to protect U.S. forces or develop a plan to deny an enemy's access to EMS.

These subsets of EW often mutually support each other in operations. For example, radar jamming (electronic attack) can serve a protection function for friendly forces to penetrate defended airspace; it can also prevent an adversary from having a complete operating picture. EW may attack and defend the EMS using cyber capabilities, while cyber operations may target parts of the EMS that are vulnerable to EW.

Differences and Overlap

Part of the convergence involves not just similarities in technical capabilities, but also cyberspace operations being used to provide EW effects, and vice versa. Cyberspace operations attempt to deny an adversary access to their computer networks using software and computer codes. EW affects communications between networks using radio jamming or other spectrum controls, while cyber operations use computer code to provide a range of effects from disruptive (e.g., denial of service attacks) to destructive (e.g., physically damaging computer components and platforms).

The most recognizable convergence of electronic warfare and cyberspace operations is when forces transmit computer code to inject it into an adversary's network. In these types of operations, radios can transmit data packets

on Wi-Fi networks, even if these networks are closed (i.e., not connected to the internet). Similarly, if an adversary operates a closed wired network, forces can potentially tap into the connections and listen to transmissions or even plant nefarious applications.

Figure 1. EC-130H Compass Call

Source: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104550/ec-130h-compass-call/.

Notes: The EC-130H Compass Call is normally used to jam enemy radars and communications. However, in recent years it has been used to transmit computer code to wireless devices using radio frequencies.

Both CO and EW can affect space operations. Satellites are controlled using ground control systems that rely on computers to maintain orbit parameters and direct onboard sensors, particularly to maintain stable orbits; radios transmit computer commands to the satellites. Computer code transmitted directly to satellites in orbit can potentially allow remote control of the system, preventing others' access to onboard sensors or communications systems. Adversaries could similarly enter ground control systems and issue alternative orders to satellites to move them out of position or shut off critical systems. Because satellites routinely receive commands using radio frequencies, an adversary might attempt to shut off sensors or directly gain control of the spacecraft, rather than trying to issue orders through a ground control system.

Cyberspace operations can also affect the electromagnetic spectrum. Active electronic scanned array (AESA) radars (which allow thousands of radio beams to transmit at once) and software defined radios (which transform how a radio wave is transmitted) rely on computer systems to manage spectrum operations. Software can help shape how these radios transmit, potentially making it difficult for an adversary to either detect or intercept radio or radar transmissions. Changes to the software can easily transform a radar or radio from a receiver to a transmitter. Having small, adjustable arrays allows AESA radars, in particular, to focus small beams of radio energy on potential targets. Radio systems like the multifunctional advanced data link on the F-35 Lightning II or the intra-flight data link on the F-22 Raptor communicate with each other by transmitting intelligence and targeting information seamlessly, while limiting their electromagnetic signature to prevent adversaries from detecting or intercepting their communications.

Operations in the Information Environment

Recognizing the importance of information superiority in military conflict, DOD's Joint Publication 1 recently named information as a seventh joint function (along with command and control, intelligence, fires, movement and maneuver, protection, and sustainment). In 2010, cyberspace was designated as a global warfighting domain that exists within the information environment, which in turn is defined as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Operations in the information environment attempt either to limit or distort a potential adversary's access to information, thereby limiting their situational awareness and potentially altering adversary decisions. CO and EW are both tools to achieve these ends. Yet, the activation of U.S. Cyber Command and the creation of a national cyber mission force may have had the effect of separating cyberspace operations as conceptually and operationally distinct, focusing more on the use of hardware and software to create effects rather than controlling information itself. While some organizations within DOD have folded former EW functions under a new cyberspace directorate and refer to "cyberspace electromagnetic activities," such integration remains inconsistent across the services. Given that the 2018 National Defense Strategy emphasizes information warfare and the integration of information as an element of national power, some military analysts argue that a new, unified Information Warfare Command may be able to remove operational stovepipes that exist between EMS and cyberspace operations, particularly as both cyberspace and the electromagnetic spectrum exist as dimensions of the information environment.

CRS Products

CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary

CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary

CRS In Focus IF11155, *Defense Primer: Military Use of the Electromagnetic Spectrum*, by John R. Hoehn

Other Resources

DOD. Joint Publication 3-12, *Cyberspace Operations*, February 5, 2013.

DOD. *The Department of Defense Cyber Strategy,* September 2018.

DOD. Joint Pub. 3-13.1, Electronic Warfare, Feb. 8, 2012.

DOD. DOD Directive 3222.04 Electronic Warfare Policy, March 26, 2014, with Change 2, Effective August 31, 2018.

Catherine A. Theohary, ctheohary@crs.loc.gov, 7-0844
John R. Hoehn, jhoehn@crs.loc.gov, 7-9074

IF11292