Blurring the Lines: The Overlap Between Cyber and Electronic Warfare

By Matt Thompson

Cyber is the buzz word of the moment. It appears to be everywhere, in all things, all the time. Cyber Attacks! Ransom Attacks! The number of jobs open in the cyber arena is staggering. Performing a quick job search for “Cyber Security” on a popular job-hunting website revealed more than 20,000 jobs actively hiring. There have even been instances where “cyber” is starting to bleed over into electromagnetic warfare (EW). This is an interesting phenomenon as cyber warfare and EW are very different animals. A great place to begin understanding these overlaps and burring is to briefly understand what each one is.

Cyber Warfare
Cyber warfare generally refers to the use of digital attacks to target computer systems, networks, and digital infrastructure. There are multiple ways to attack including actions like hacking into networks, spreading malware, conducting denial of service attacks, and disrupting or manipulating information. The objective is often to steal, alter, or destroy data, disrupt operations, or spread propaganda.
This description can help one visualize the possible benefits in a warfare environment. With that in mind, Cyber warfare is not EW, or is it? Let’s refresh what EW is.

Electronic Warfare (EW)
EW involves the use of the electromagnetic spectrum (radio waves, radar, etc.) to detect, intercept, and jam enemy communications and radar signals. It can also involve

protecting one’s own electronic equipment from similar attacks. The main components of EW are electronic attack (EA), electronic protection (EP), and EW support (ES).
A further breakdown is to understand the domains where these types of operations occur, what some of the pathways of attack are and how the objectives differ.

Domain of Operation
Cyber Warfare: Primarily operates in the digital domain, targeting computer systems, networks, and digital infrastructure.
Electronic Warfare: Operates in the electromagnetic spectrum, targeting communication and radar systems.

Tools and Techniques
Cyber Warfare: Malware, ransomware, phishing, distributed denial-of-service (DDoS) attacks, etc.
Electronic Warfare: Jammers, interceptors, decoys, and detectors.

Objective
Cyber Warfare: Disrupt operations, steal/alter/destroy data, or spread misinformation.
Electronic Warfare: Disrupt or intercept enemy communications and radar, while protecting one’s own systems.

This now starts to highlight some areas where the overlap occurs. Maybe it is tactically advantageous to use cyber and EW together? For instance, a cyber-attack might target the software of a radar system, while EW might jam the radar’s signals. Both aim to disable the radar, but they approach the problem from different angles. The question is if one is more effective than the other? Is the overall result better if both techniques are used simultaneously? In modern warfare it is easy to see why the lines between cyber and EW are blurring. The lines might be blurring but the distinctions remain.
While both cyber and EW target and defend systems, their primary domains and methods are distinct. Cyber warfare is

more about the software and data, while EW is about the hardware and signals. Looking to the future, the lines will continue to blur as technology evolves, despite the distinctions of intent.

Here are a few potential future intersections:
Integrated Systems: Modern military systems often integrate both electronic and cyber components. An attack on one can affect the other.
IoT and Smart Devices: As more devices become interconnected, the potential for cyber attacks to have electronic consequences (and vice versa) increases.
AI and Automation: With the rise of AI-driven warfare, both cyber and EW tools might be used in tandem to confuse, disable, or take over automated enemy systems.
Space Warfare: Satellites and other space assets rely on both electronic systems for communication and computer systems for operation. Attacks in space might combine elements of both cyber and EW.

While cyber warfare and EW have distinct origins and methods, the increasing integration of electronic systems and computer networks means that they will likely become more intertwined in the future. However integrated these two critical missions become, they remain distinct. It is important to not overly confuse them to ensure both have the proper authorities and necessary resources to achieve and sustain an advantage in the invisible battlespace of the electromagnetic spectrum. We have significant and persistent shortfalls in EW that we need to address throughout the Department of Defense and across the military services, especially in workforce development and readiness. Hopefully, in the years to come we will realize that we too have 20,000 open jobs in EW and we need to start filling them today.