Blurring the Lines More… (Another Perspective)

By Matt Thompson

In October 2023, I wrote an article in AOC's eCrow newsletter about the blurring of lines between Electromagnetic Warfare (EW) and Cyber. I happened to revisit another article published in C4ISRNet a few years back in 2021 that influenced me to start thinking about this topic again. It was an interesting perspective that the blurring of the lines was intentional with concepts like RF-enabled cyber.

To delve deeper into this confluence of cyber warfare and EW, a perspective offered in the C4ISRNet article highlights a strategic pivot by the US military towards blending these domains. This integration signifies a recognition of the evolving battlefield, where the lines between cyber and EW continue to blur, fostering a new realm of tactical advantages and operational challenges.

The Evolution of Warfare: Blending Cyber and EW
Modern warfare is increasingly characterized by the integration of cyber capabilities with traditional EW operations. This strategic fusion aims to exploit the full spectrum of the electromagnetic domain, enhancing the US military's ability to operate and dominate in contested environments. As adversaries advance their technologies, the US response by merging cyber and EW efforts represents a pivotal adaptation to maintain superiority.

Strategic Integration and Operational Synergies
The C4ISRNET article underscores the US military's initiative to create more cohesive and integrated frameworks for cyber and EW operations. This approach not only streamlines command and control but also maximizes the effectiveness of both

domains. By operating in tandem, cyber attacks can be synchronized with electronic attacks, creating multifaceted challenges for adversaries that are harder to predict and counter. This synergy enhances the ability to disable or manipulate enemy systems through a combination of software vulnerabilities and electromagnetic disruption.

Challenges of Integration
However, the integration of cyber and EW also presents unique challenges. One primary concern is the need for personnel skilled in both disciplines. As technology evolves, the demand for professionals capable of navigating the intricacies of both cyber and electronic spectrums becomes critical. The distinction between cyber warfare, focused on software and data, and EW, targeting hardware and signals, necessitates a nuanced understanding and approach to warfare that blends these aspects seamlessly.

Future Intersections: A Roadmap
Looking ahead, several potential intersections between cyber warfare and EW are poised to redefine the landscape of military operations:

- **Integrated Defense Systems:** The integration of cyber and EW capabilities into defensive systems can provide a more robust mechanism for identifying, tracking, and neutralizing threats. This could mean using cyber tools to enhance electronic defenses or vice versa, ensuring a comprehensive protective net against a wide range of attacks.
- **Autonomous Systems and AI:** I have mentioned it before, but the role of artificial intelligence (AI) in future warfare cannot be overstated. AI-driven systems, empowered by cyber and EW capabilities, could lead to highly autonomous, self-coordinating defense mechanisms. These systems could preemptively identify threats and deploy countermeasures without human intervention, marking a significant shift in how operations are

conducted. I also highlighted this autonomous nature as a risk, as I believe there will always need to be some sort of man in the loop decision making.

- **Space and Cyber-Electronic Warfare:** The final frontier is increasingly becoming a contested domain, with satellites and other space assets playing critical roles in global communications, navigation, and surveillance. The integration of cyber and EW capabilities in space warfare offers the potential to protect these assets from sophisticated attacks or, conversely, to disable enemy assets through a combination of cyber intrusions and electronic jamming.

Addressing Shortfalls and Preparing for the Future

Despite the potential, significant shortfalls in EW capabilities and readiness must be addressed to fully realize the advantages of integrating cyber and EW. Workforce development is a critical area of focus, with a pressing need to cultivate a new generation of professionals skilled in both cyber and electronic domains. Just as there is a notable surge in cyber security job openings, a similar emphasis on developing EW talent is imperative.

As the US military endeavors to blend cyber and EW capabilities, it is crucial to maintain clarity on the distinct but complementary nature of these domains. This distinction ensures that strategic focus and resources are adequately allocated to develop and sustain capabilities in both areas. The goal is to achieve and maintain a tactical advantage in the increasingly complex and invisible battlespace of the electromagnetic spectrum.

In conclusion, the integration of cyber warfare and electronic warfare represents a strategic evolution in modern military operations. As these domains become increasingly intertwined, the challenges and opportunities presented will shape the future of warfare. Addressing current shortfalls, particularly in workforce development and readiness, will be crucial to

capitalizing on the potential of this integration. The journey towards a seamless blend of cyber and EW capabilities will undoubtedly redefine the contours of global security and defense strategies in the years to come.