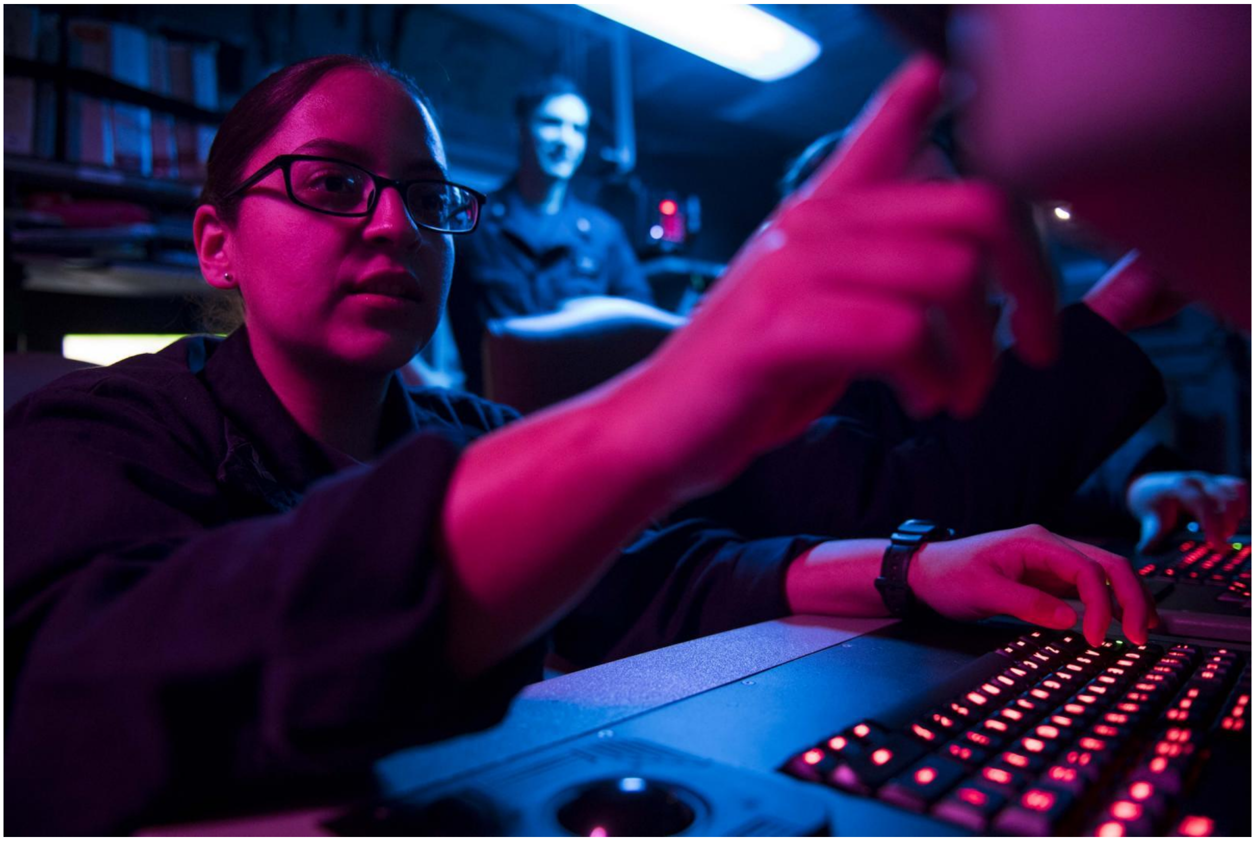

Build a True Navy Cyber Corps

The Navy should merge its information professional and cryptologic warfare communities into a true cyber corps that is competent in both cyber defense and offense.

By Lieutenant Commander Travis Howard, U.S. Navy

May 2019
Proceedings | Vol. 145/5/1,395

The Director of National Intelligence has placed cyber at the top of global threats the United States and its allies face.[1] The assessment demonstrates how cyber operations and employment of information technology (IT) by U.S. "adversaries and strategic competitors" are inextricably linked, and how these nations manipulate the proliferation of IT and electromagnetic spectrum ecosystems to their operational advantage.[2] The U.S. Navy is charged with engaging these adversaries in cyberspace, both jointly and in the maritime domain, and requires a full-spectrum approach to achieve results. This reality is described well in a recent Center for International Maritime Security article: "Cyberspace and the Electromagnetic Spectrum are material realizations of the information domain, whether midpoint or endpoint, Internet Protocol or radio frequency, defense or attack, this is where you fight, for there is only one network separated in time."[3]

Today, two of the four Navy officer designators within the information warfare (IW) community have primary responsibilities for cyber warfare and electromagnetic warfare (EMW). Cryptologic warfare (CW) officers, trained as signals intelligence (SigInt) experts and manipulators of the electromagnetic spectrum, recently assumed the leading role in Navy cyberspace operations. Information professional (IP) officers manage the Navy's enterprise network and communications (management of the electromagnetic spectrum) infrastructure, to include taking a lead role in cybersecurity. Yet the expertise these two officer communities bring could be better optimized to support Navy operational concepts such as distributed maritime operations if they are merged to create a cadre of operationally-focused technical specialists and leaders—a true Navy cyber corps. In no other Navy warfare community—submarine, surface, aviation, special warfare—are the responsibilities for "offense" and "defense" so stringently segregated into separate officer communities.

Aligning Critical Cyber Expertise

Aligning CW and IP skills into under one cyber corps officer designator would enhance Navy warfighting talent in the information environment and provide a focused team effort to achieve operational effects in cyberspace. CW and IP officers have similar educational backgrounds and skills to competently manage warfare in the electromagnetic spectrum and both offensive and defensive cyber operations. One cyber corps that develops officers with expertise in terrestrial and satellite communications, information technology management, and offensive and defensive cyber operations would enable the Navy to operate emerging, disruptive technology and services such as data analytics, cloud computing and applications, cybersecurity infrastructure tools, and mobility solutions not just from a technology management perspective, but with an eye toward conducting asymmetric IW at the tactical and operational levels of war.

CW officers, with their cyber and EMW background, can succeed in IP billets with IP-based foundational training (many of them already have the academic qualifications), while IP officers could significantly enhance their warfare skills and be better communicators, operators, and tactical watchstanders by acquiring CW skills. IP officers and the enlisted IT rating are already skilled in terrestrial and satellite communications management, network system administration, maintenance, and troubleshooting. With the additional insight gained by a deeper understanding of how the Navy operationalizes the electromagnetic spectrum, these officers and technicians could be even more proactive enablers of missions in all domains where cyber and EMW have critical roles.

In military planning, it is often said that "the enemy gets a vote." This is particularly the case in the cyber domain. In 2016 a conference of Pentagon leaders, military academy professors, and industry "white-hat" hackers came to four key conclusions about the cyber domain: You can't teach defense without understanding offense; operating in the cyber domain is all about breaking the rules; there is no “high ground;” and the weapon you have today may not exist tomorrow.[4] With much of the Navy's offensive cyber expertise residing in the CW community, and the system administration expertise in the IP community, it is evident a fractured approach will not work in the long run.

Combining CW and IP expertise into a single cyber corps could produce an agile force better positioned to operate across the competition-to-conflict spectrum as outlined by Chief of Naval Operations Admiral John Richardson in his “Design for Maintaining Maritime Superiority (Version 2.0).” The return of great power competition and the codification of the IW community demands Navy personnel become more technologically agile to compete in high-end conflict.[5]

The Cyber Corps Afloat

A cyber corps would better support the other Navy warfare areas. In surface warfare, for example, distributed maritime operations that rely on fast-reacting surface action groups is a resurgent concept.[7] Cyber corps officers serving as the Ship’s Signals Exploitation Space (SSES) or communications division officers, both with a thorough understanding of EMW and communications, could more effectively work in tandem to rapidly inform the commanding officer on how the ship’s operations could be enhanced—or hindered—by electromagnetic effects and the efforts of the adversary to deny or degrade communications. They also could tailor communication planning to the ship’s or surface action group’s EMW plan far better than can be currently done by the separate communities.

The Navy has recently made significant improvements in IW doctrine, demonstrating a desire to evolve old but conceptually sound constructs to the new demands of IW. The year 2018 was important for the Navy’s IW community as it established the IW commander afloat as a post-command, screened, and cross-detailed “best of the best” warfare billet on carrier strike group and amphibious ready group staffs. To that end, the Navy established the Information Warfare Training Group to improve training and the Naval Information Warfare Development Center to develop tactics and drive IW innovation.[6] A cyber corps will take full advantage of these improvements and provide IW commanders afloat with a more competent talent pool of officers capable of both maintaining complex command and control (C2) networks as well as delivering networked effects.

Imagine a cyber corps officer standing watch as a shipboard tactical action officer. The knowledge he or she possesses in signals intelligence and electronic warfare (the work in the SSES), coupled with in-depth knowledge of the ship’s communication and network operations capabilities (the ship’s radio and advanced data processing spaces), would be a powerful asset for the commanding officer. Steeped in maritime operations, that officer has the potential to be one of the strongest tactical watchstanders afloat, whether part of ship’s company or embarked staff.

The IW commander would take advantage of a fully synergized cyber, communication, and electronic warfare officer community under the distributed maritime operations concept, where every billet matters and any officer regardless of paygrade can make a sizable contribution. The cyber corps would fill both the strike group communications officer (N6) billet and cryptologic resource coordinator (N21 or N22) billet, and—by virtue of being from the same specialized community—these officers would collaborate better in developing a threat-informed communication plan and operational tasking for distributed forces.

Challenges and Opportunities

The alignment of CW and IP expertise into a cyber corps presents many challenges and opportunities for the Navy. Make no mistake—this would be a disruptive process, and some china will break. Billet structures would have to be redesigned, training commands merged and curricula consolidated, and the supporting enlisted workforce realigned to meet the needs of this new community. These efforts could be accelerated by rethinking how the Navy recruits and trains for warfare in the cyber domain. The Navy's revolution in "ready relevant learning" would be key in shaping training pipelines to keep the best while jettisoning the rest.[7] Enlisted specialties in both the cryptologic warfare and information systems technician ratings could benefit from a tighter alignment. The Navy has already begun to group some of these ratings, with IT and cryptologic technician-network (CTN) ratings now grouped as "cyber" within the IW community.[8] The fiscal challenges of such a massive change to workforce and training requirements would be significant but not insurmountable, particularly in light of the Navy's potential adversaries and their focus on building cadres of highly specialized cyber warriors.

Adapting and Responding with Urgency

Hyperconverged information processing and data storage, artificial intelligence, autonomous systems, and the need for focused intelligence informing cyber operations are significant cyber domain trends that require the Navy to "upset the apple cart" in the IW workforce. Such change won't water down existing CW and IP core competencies. If done smartly, the best of both worlds will be realized with a rich cadre of best-in-class expert IW resource managers and technical leaders to lead the phenomenal IT and CT enlisted rating talent.

Cultural naysayers should not be allowed to stand in the way of progress that would benefit the Navy. Bold and decisive leadership is needed now to shape the workforce that will enter the fight tomorrow. The sense of urgency in "Design 2.0" is evident, and Navy leaders clearly understand the danger of falling behind. Now is the time to take another important step to demonstrate the Navy's adaptability and harness the power of the information age.

Special thanks to several colleagues who helped shape this article.

1. Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," 29 January 2019.

2. Coats, "Worldwide Threat Assessment," 5.

3. VADM T.J. White, RDML Danelle Barrett, and LCDR Robert “Jake” Bebber, “The Future of Information Combat Power: Winning the Information War,” Center for International Maritime Security (CIMSEC), 14 March 2019.

4. Tobias Naegele, “Hackers to Pentagon: You’re Doing Cyber Wrong,” *Nextgov.com*, 19 January 2016.

5. ADM John Richardson, “Design for Maintaining Maritime Superiority, Version 2.0,” December 2018.

6. Gidget Fuentes and Megan Eckstein, “Navy Information Warfare Effort Set to Expand, Evolve,” *USNI News*, 7 February 2018.

7. U.S. Fleet Forces Command, “Vision and Guidance to Ready Relevant Learning,” August 2017.

8. Chief of Naval Operations, “NAVADMIN 174/17: Revised Navy Enlisted Classification Code Construct,” 13 July 2017.