

Develop Separate Navy Cyber and Signal Warfare Communities

Christopher B. Landis
July 2022

Proceedings

Vol. 148/7/1,433

FEATURED ARTICLE

The Navy is not optimally structured for cyber operations and electromagnetic maneuver warfare.

Over the past few years, several *Proceedings* authors have suggested improving the Navy's cyber operations and electromagnetic maneuver warfare (EMW) capability by reorganizing the pertinent communities within the information warfare community (IWC). One author proposed combining the cryptologic warfare (CW) and information professional (IP) communities.¹ Others recognized that cyber operations are too much for any one community and that EMW is its own career field, requiring education and experience to build a proficient cadre.² Their proposals were well written and sought the betterment of the Navy; however, they failed to identify and address the root cause of the shortcomings they all reported.

The root cause of the symptoms driving these proposals is a lack of efficient alignment of cyber and EMW in the IWC. About half the active-duty IWC CW and IP personnel alternate between operating, defending, and exploiting the cyber domain and operating, defending, and exploiting the electromagnetic spectrum.

Consider a CW officer serving her first tour with the Cyber National Mission Force and her second tour as a ship's signals exploitation division officer. This standard CW junior officer career path results in the officer's skills in one area—cyber—growing stale while she works in the electromagnetic spectrum. Furthermore, those who exploit a domain and operate in it consistently are better poised for success than those who either exploit both or operate in both. For this reason, the CW and IP communities should be realigned as signal warfare and cyber warfare communities.

Current Organization and Functions

TABLE 1

Comparison of Current CW and IP Competencies		
Competency	CW	IP
OCO	X	
DCO-RA	X	
DCO-IDM		X
DoDIN Ops		X
EW	X	
SIGINT	X	
Radio Frequency Communications		X
Spectrum Management		X
Combat Systems		X
Space		X
Knowledge Management		X
Chief Information Officer		X

Cryptologic warfare officers and cryptologic technicians. As a Navy IW profession, cryptology has a more than 80-year rich history. Although its mission has evolved over the years, today it “encompasses signals intelligence, cyberspace operations, and electronic warfare operations in order to deliver effects through sea, air, land, space and cyber domains at all levels of war.”³ There are five branches within the enlisted cryptologic technician (CT) rating—interpretive (CTI) for linguistics, maintenance (CTM) for cryptographic equipment maintenance, network (CTN) for cyber operations, collection (CTR) for signals intelligence (SigInt), and technical (CTT) for electronic warfare (EW).⁴

Information professional officers and information system technicians. The Navy created the IP community in 2001. It includes six core competencies:

- Cyber network defensive and offensive operations
- Radio frequency and telecommunications operations and maintenance, including spectrum management
- Combat systems operations and maintenance
- Space

- Knowledge management
- Chief information officer functions⁵

TABLE 2

Proposed Organization of Cyber and Signal Warfare Communities		
Competency	Cyber Warfare	Signal Warfare
OCO	X	
DCO	X	
DoDIN Ops	X	
EW		X
SIGINT		X
RF Communications		X
Spectrum Management		X
Combat Systems	Information Networks	Radars and Weapons
Space	Computers on Satellites	Communications and SIGINT
Enlisted Rating Alignment within the Proposed Warfare Communities		
	CTN, IT, ITS	CTI, CTM, CTR, CTT, RM ^a

^a The radioman (RM) rating does not currently exist.

Comparing this core competency list with older versions and earlier definitions of the IP community clearly shows the rapid growth of the community into its crucial role in the Navy. The information technician (IT) rating supports all these competencies but is largely spread between radio systems and automated data processing (computer network) systems.⁶ Relatively few ITs master both fields.

Although both the CW and IP communities claim the full spectrum of cyber operations in their community descriptions, in practice there is a distinct divide in roles (see Table 1). While the CW community focuses more on offensive cyberspace operations (OCO) and defensive cyberspace operations–response actions (DCO-RA), and the IP community focuses more on DCO-internal defensive measures and Department of Defense information network (DoDIN) operations, both communities have a few billets in the opposite areas. From the perspective of electromagnetic spectrum signals, the CW community focuses more on exploiting signals and the IP community focuses more on using and managing signals.

Risk to Mission

The Navy IWC's organizational structure is vulnerable in supporting cyber operations and EMW. In both the CW and IP communities, service members—specifically CW officers, IP officers, and ITs—often alternate between cyber-related jobs and signals-related jobs. (The branches within the CT rating largely keep them aligned within either cyber or signal.) While this is ostensibly good for developing well-rounded sailors, it will not help develop the most effective cyber operations or EMW workforce.

TABLE 3

Sample Billet Recoding Supporting the IWC Reorganization				
AIRCRAFT CARRIER				
Division Name	Officer		Enlisted	
	Current	Proposed	Current	Proposed
Automated Data Processing	IP	Cyber	IT	IT
Communications Security (Crypto Management)	IP	Either	IT	IT/RM
Cybersecurity	IP	Cyber	IT	IT
DCO (embarked)	None	Cyber	CTN	CTN/IT
Electronic Warfare	Varies	Signal	CTT	CTT
Main Communications (Radio)	IP	Signal	IT	RM
Ship's Signals Exploitation	CW	Signal	CTM/CTR	CTM/CTR
Naval Computer and Telecommunications Station				
Circuit Actions/Tactical Plans	IP	Signal	IT	RM
DCO	IP	Cyber	IT	CTN/IT
Enterprise Network Services	IP	Cyber	IT	IT
Fleet Network Operations Center	IP	Cyber	IT	IT
Information Assurance	IP	Cyber	IT	IT
Joint Fleet Telecommunications Operations Center	IP	Both	IT	IT & RM
Message Processing Center	IP	Either	IT	IT/RM
Satellite Communications Facility	IP	Signal	IT	RM
Technical Control Facility	IP	Signal	IT	RM

The Secretary of the Navy March 2019 *Cybersecurity Readiness Review* recognized that people are the Navy's greatest asset and liability.⁷ Who knows how to attack a vulnerable system more than the expert at defending it? Many carrier strike group information warfare commander postdeployment reports state that the lack of a system-administrator-experienced IT on the DCO augmentation team hampered the team's effectiveness. Similarly, the 2020 DoD *EMS Superiority Strategy* expressed the need to have experts in maneuvering within the contested electromagnetic spectrum, whether in conflict or peacetime.⁸

A New Organization

To overcome the lack of integration and synchronization that currently exists (outside of U.S. Cyber Command and its components) in the IWC, the CW and IP communities should be restructured and renamed, as depicted in Table 2.

Competencies traditionally called combat systems and space are adapted in this organization to their evolving technologies. Combat systems is headed more toward applications on information networks. The proposed cyber warfare community would be best positioned to secure, operate, defend, fight, and maintain these combat systems. At the same time, the proposed signal warfare community knows the electromagnetic spectrum environment and its threats and would be the best at configuring and operating the radars and weapon systems that depend on the electromagnetic spectrum. This is also true for space systems. Modern computers on satellites often function just like computers on Earth, thus simply extending the computer network physically. The principles of communications and SigInt in space are like their terrestrial communication counterparts.

For the enlisted ratings, those that deal specifically with cyber operations would become part of the cyber warfare community. Besides CTN, all other CT branches are better suited to become part of the signal warfare community. The ITs, according to their current specialties, span both proposed communities. To alleviate the stress of spreading the IT rating too thin, the radioman (RM) rating, which merged into IT in November 1999, would be reestablished.⁹ Pulling the RM rating back out of the IT rating would enable IT and RM technicians to deepen their knowledge of cyber operations and signal warfare without having to be experts in both fields.

Expanding the IWC to include the electronics technician (ET) rating—specifically those technicians that have the naval enlisted classifications (NECs) for computer networks (cyber), radios (signal), and radars (signal)—is also a consideration but must be studied in more depth. ETs have contributed significantly to information warfare but are not yet recognized as IWC members.

Implementing the New Organization

Restructuring the IWC as described would not require creating or eliminating IWC billets. Instead, each CW and IP billet would be recoded and filled by one of the new communities, involving coordination with each type commander that resources CW and IP billets. Table 3 includes two examples from my career history—an aircraft carrier and a naval computer and telecommunications station.

To implement this organizational restructuring, the Navy would need to determine the criteria for sorting its CW and IP officers and ITs into the new communities. One recommendation would be to offer everyone the opportunity to submit his or her preference. Based on the billet base per new community per paygrade compared with the preferences they submit, the Navy would only need to address those specific paygrades and communities for which the demand to join did not match the number of billets. The Navy could determine who would join which community via a service record review of those affected. This could be based on jobs performed, Navy enlisted classification, Navy officer billet classification, or additional qualification designation codes.



A radioman seaman assigned to the Sixth Fleet staff on board the guided-missile cruiser USS Belknap (CG-26) in December 1989. Reestablishing the radioman rating and pulling it out of the IT rating would enable IT and RM technicians to deepen their knowledge of cyber operations and signal warfare without having to be experts in both fields. Credit: Naval Institute Photo Archive

Alternatively, the Navy could simply decide and assign officers and sailors based on the service record review. Officers and sailors assigned contrary to their personal preference could request a lateral transfer (officers) or rating conversion (enlisted) in accordance with existing procedures. There may be unusually high demand for lateral transfer or rating conversion immediately following the reorganization. This would be a significant and potentially controversial shift in the IWC. There will be growing pains associated with this change.

Regarding the enlisted rating names, for now they should remain the same. Eventually, changing the rating names to align with the communities will probably be necessary. Sailors are proud of their ratings. Therefore, it is important the Navy take a measured approach to any rating name changes.¹⁰

The importance of investing in sailors over warfighting systems is clear: "Sailors are the most modular, lethal, and adaptable asset the Navy has."¹¹ Improving cyberspace operations and electromagnetic maneuver warfare capabilities in the Navy requires focusing on sailors and organizing them into a more effective community structure so their training will be more relevant for longer and their enhanced expertise will increase the Navy's lethality and reduce risk to its missions. Effectively realigning the IWC will pay far greater dividends than initiatives such as increasing career field bonuses to improve retention.¹² Repeatedly having to relearn one's trade at each duty station diminishes readiness, but also sailor job satisfaction and retention.

Imagine the radio technician and the signal exploiter in the same community working together to maneuver dynamically within the electromagnetic spectrum during a high-end fight. Likewise, imagine the information systems administrator adjusting the network's cyber protection posture to maintain mission-essential availability in conjunction with an offensive cyber operation. Reorganizing the IWC into cyber and signal warfare communities is the right next step to improve the Navy's information warfare profession.

References

1. LCDR Travis Howard, USN, "Build a True Navy Cyber Corps," U.S. Naval Institute *Proceedings* 145, no. 5 (May 2019).
2. LCDR Derek S. Bernsen, USNR, "Navy Cryptologic Warfare Officers Cannot Do Cyber," U.S. Naval Institute *Proceedings* 148, no. 1 (January 2022); CDR Tam N. Pham, USN, "Elevate EMW Education," U.S. Naval Institute *Proceedings* 145, no. 5 (May 2019); and LTJG Brandon Karpf, USN, "Train Navy Officers for Cyber Lethality," U.S. Naval Institute *Proceedings* 145, no. 2 (February 2019).
3. VADM Jan E. Tighe, USN, *Navy Cryptologists: Leaders Across the Spectrum* (Washington, DC: Department of the Navy, 25 June 2016).
4. Tighe, *Navy Cryptologists: Leaders Across the Spectrum*.
5. U.S. Naval Personnel Command, Bureau of Naval Personnel, *Information Professional (IP) Officer Senior Detailer, Information Professional Officer Career Handbook* (Millington, TN: July 2016), iv.
6. Commander, Naval Network Warfare Command, *Community Indoctrination for Information Professional Officer* (Suffolk, VA: 19 June 2007), 6.
7. HON Michael J. Bayer, John M. B. O'Connor, Ronald S. Moultrie, and William H. Swanson, *Secretary of the Navy Cybersecurity Readiness Review* (Washington, DC: 4 March 2019), 17.
8. HON Mark Esper, *Department of Defense Electromagnetic Spectrum Superiority Strategy* (Washington, DC: October 2020), 3–4.
9. Navy Information Systems Technician, Navy CyberSpace (navyncs.com), 11 September 2018, www.navyics.com/navy-jobs/information-systems.html.
10. Mark D. Faram and David B. Larter, "Ratings Restored: Effective Immediately, Sailors Will Get Their Job Titles Back," *Navy Times*, 20 December 2016.
11. LT Brendan Cordial, USN, "People Over Payloads," U.S. Naval Institute *Proceedings* 144, no. 5 (May 2018).
12. LCDR Dusty McKinney, USN, "Navy Cyber Needs a Refit," U.S. Naval Institute *Proceedings* 148, no. 2 (February 2022).