Center for International Maritime Security

CYBER WAR

NAVY CULTURE MUST BE ADAPTED TO FIT THE INFORMATION AGE

JUNE 18, 2019 | TRAVIS HOWARD | 3 COMMENTS

By Lieutenant Commander Travis D. Howard, USN

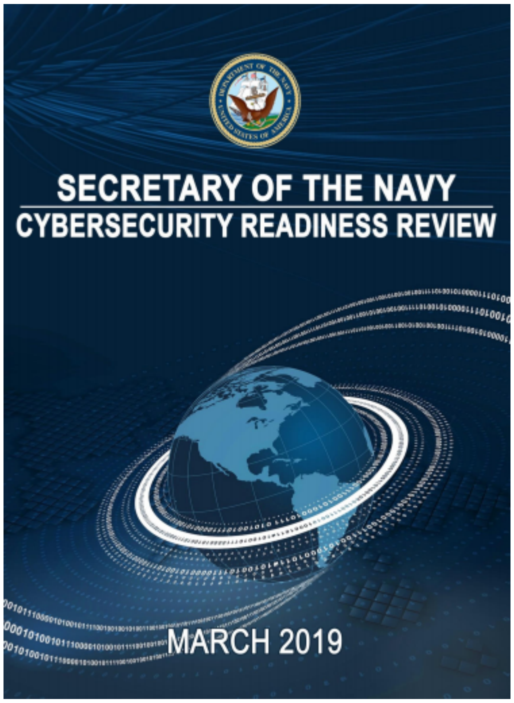
A recent independent review of the Navy's cybersecurity posture, completed in March 2019, was predictably harsh on our Navy's current culture, people, structure, processes, and resourcing to address cybersecurity.[1] For many of us within the Information Warfare discipline, much of this report does not come as a shock, but it does lay bare our cultural, structural, and procedural problems that the Navy has been struggling with since the turn of the century.

The 76th Secretary of the Navy, Richard V. Spencer, should be applauded for enabling open and honest dialogue on the key issues of this report by releasing it for public comment and professional discourse. The review found that the Navy was not "optimally focused, organized, [nor] resourced" for cyberwar.[2] Such transparency has been the hallmark of the naval service for centuries, and is largely the reason why such robust professional forums such as the United States Naval Institute (USNI) and the Center for International Maritime Security (CIMSEC) continue to thrive.

The report was particularly critical of the Navy's culture, stating that the Navy is "preparing to win some future kinetic battle, while it is losing the current global, counter-force, counter-value, cyberwar."[3] The report goes on to recommend that the highest levels of Navy leadership adjust the service's cultural landscape to become more information-centric, rather than platform-centric. This excerpt is particularly vexing:

"Navies must become information enterprises who happen to operate on, over, under, and from the sea; a vast difference from a 355 ship mindset."[4]

In truth, the Navy that acts as an information enterprise and the Navy that pursues the tenants of traditional naval warfare as laid out by naval doctrine are not mutually exclusive. Our drive toward a bigger, better, and more ready Navy, aligned to the National Defense Strategy, requires a naval culture ready for high-end conflict but active and engaged in all levels of conflict below lethal combat. The adoption of information enterprise core principles certainly has a place in our doctrine; in fact, it's already there but lacks proper execution and widespread cultural adoption as a core competency across all warfare communities. Navy culture can be adapted to better fit the information age, but it will take the entire Navy to do it and not just a single community of effort.



Information is Already in our Doctrine, but Prioritization Must Improve

The 31st Chief of Naval Operations (CNO), Admiral John Richardson, released a *Design for Maintaining Maritime Superiority* shortly after assuming his role, and recently released an update (*Design* 2.0) to compliment the 2018 National Defense Strategy. The CNO put information warfare at the center of his strategic thinking, and challenged the Navy's operational and resourcing arms to "adapt to this reality and respond with urgency."[5] But this change in the security environment wasn't new to this CNO, in fact, it was foreseen decades ago by thinkers like CAPT (ret.) Wayne P. Hughes, a venerated naval tactician and professor emeritus at the Graduate School of Operations and Information Sciences of the Naval Postgraduate School. Early versions of Hughes' *Fleet Tactics and Coastal Combat*, required reading in graduate-level naval officer training, placed information, rapid adoption of technology, and intelligence at the forefront of effective maritime operations in the modern age.[6]

If we've valued information in warfighting all along, then why are we failing to adapt our naval culture to the Information Age? The Cybersecurity Readiness Review cuts straight to the point: "… cybersecurity continues to be seen largely as an 'IT issue' or 'someone else's problem.'"[7] In our haste to stand up a community of practice to *do all the cyber things* we, as a Navy, failed to make the necessary cultural changes that should have accompanied it.

Why hasn't the growth of the Information Warfare Community focused the Navy's culture appropriately? After all, creating such specialized warfare communities has always worked well in the past, as any aviator can attest to. Truthfully, the problem is bigger than just one community; the subsequent decades saw the rise of global information technology as central to nearly everything we do, and every Sailor now uses the network as a primary on-the-job resource. The loss of email, web browsing, and support systems that handle tasks from personnel to logistics can and does result in work stoppage; any assertions to the contrary, that workarounds or manual methods still exist, do not accept the reality of the situation.

Cultural change is long overdue, and just like a Marine or Soldier learns how to handle their weapon safely and effectively from day one, we must now train and mentor our Sailors to use the network in the same vein. No more can we flippantly say "we have people for that" when faced with information management and cybersecurity problems, putting effort into modernizing complex systems and enhancing Information Warfare's lethality, while ignoring the power a single negligent user could wield to bring it all down. It's all hands on deck now, or the Navy faces the very real possibility of fumbling the opening stages of the next kinetic fight.

Security is Already an Inherent Part of Navy Culture

The good news is that information security is already an intrinsic part of being a member of the armed forces, uniformed or civil service. Security clearances, safe handling procedures for classified information, and cryptography practices like two-person integrity have been trained into the workforce for decades. Protecting information is as much a part of our culture as operating weapons systems or driving warships.

The Navy's training machine should find ways to leverage this existing culture of compliance to incorporate dynamic and repetitive ways to reach all Sailors at all stages of development – from boot camp to C school, from initial officer training to graduate school, focused on making each Sailor a harder target for information exploitation. Each engagement should be tailored to fit the environment and to complement subject matter: initial user training should teach how to report spear-phishing, practice OPSEC on social media (and how to spot adversarial attempts to collect against them), and recognizing unusual activity on a network workstation. A more senior Sailor in C-school might learn how to look at cybersecurity from a supervisory perspective, managing a work center and a group of network assets, and how to spot and report insider threats both malicious and negligent. An officer in a naval graduate program, such as at NPS or the Naval War College, would take advanced threat briefings on adversarial activity targeting rank-and-file users on the network, and how to incorporate such threat information into wargaming to inform the strategic and operational levels of war.

Some of these actions are already in the works, but the emphasis should be on how to engage Sailors in multi-faceted, multi-media ways, and repetition is critical. Seeing the same concept in different ways, in different case studies, reinforces better behavior. The Navy is no stranger to this training method: we are masters at repetitive drills to train crews to accomplish complex actions in combat. Reinforcement of this behavior cannot come fast enough. Incidents attributed to negligent network users are on the rise, and cost organizations millions of dollars a year.[8] The Navy is no exception: category-4 incidents (improper usage) are too common.

Ultimately, the objective should be a Sailor who understands cyber hygiene and proper use of the network as a primary on-the-job tool, just as well as any Soldier or Marine knows his or her rifle. Sailors go to sea aboard complex warships with integrated networked systems that run everything from Hull, Mechanical, and Electrical (HM&E) systems to combat systems and weapons employment. The computer is our rifle, why shouldn't we learn how to use it more safely and effectively?

Keys to Success

Cultural change is hard, but lessons learned from our past, best practices from the private sector, and good old fashioned invasive leadership (the kind the Navy does very well) can adjust the ship's rudder and speed before we find ourselves much further in shoal water.

Top level leadership must set the conditions for success, but they have to believe in it themselves. Our Sailors can easily tell when a leader doesn't fully commit to action, paying lip service but nothing beyond it. They are also hungry to follow a leader who has a passion for what they do. To effect change, passionate leaders need to take center stage with the authority and resources necessary to translate change into action at the deckplate level. When a Sailor sees a top-level message about a desired change, then sees that change actually happening in their workspace, it becomes real for them. Let's also trust them to understand the threats, rather than keeping the "scary" threat briefs at the senior levels.

Successes must be celebrated, but failures must have real consequences. It's time to get serious about stopping insider threats, specifically negligent insiders. Too often the conversation about insider threats goes to the criminal and malicious insiders, ignoring the most common root of user-based attack vectors. Our Sailors must be better informed through regular threat briefings, training on how to spot abnormal activity on the network, and clear, *standardized* reporting procedures when faced with phishing and other types of user-targeted attacks. Those who report suspicious activity resulting in corrective action should be rewarded. Likewise, those who blatantly ignore established cyber hygiene practices and procedures must face real consequences on a scale similar to cryptographic incidents or unattended secure spaces. This will be painful, but necessary to set our user culture right.

Effective training begets cultural change. We must take advantage of new and innovative training methods to enrich our schoolhouses with multimedia experiences that will reshape the force and resonate with our new generation of Sailors. The annual Cybersecurity Challenge should be retired, its effectiveness has been questionable at best, and replaced with the same level of rigor that we used to attack no-fail topics like sexual assault prevention. With the stand-up of a Director of Warfighting Development (N7), and the lines of effort within the CNO's Design 2.0 rife with high-velocity learning concepts, the near-future landscape to make this sea change looks promising.[9]

Conclusion

The Navy has spent the better part of 30 years struggling to adopt an information-centric mindset, and the good news is that operational forces have come a long way in embracing the importance of information in warfare, and how it permeates all other warfare areas. Yet our culture still has a long way to go to break the now dangerously misguided notion that information management and cybersecurity are something that "we have people for" and doesn't concern every non-IW Sailor. The IW Community has come a long way and can do a lot to further the Navy's lethality in space, cyberspace, and the electromagnetic spectrum, but it can't fix an entire Navy's cultural resistance to change without strong assistance.

Secretary Spencer, in his letter introducing the public release of the 2019 Cybersecurity Readiness Review, noted that "the report highlights the value of data and the need to modify our business and data hygiene processes in order to protect data as a resource."[10] He highlighted that cross-functional groups were already underway to address the findings in the report, and surely the machinations of the Navy Headquarters are more than capable of making the necessary changes to the Navy's "policy, processes, and resources needed to enhance cyber defense and increase resiliency."[11] But culture, that's all of us, and we must be biased toward change and improvement. We are the generation of naval professionals who must adapt to this reality and respond with urgency.

Lieutenant Commander Howard is an Information Warfare Officer, information professional, assigned to the staff of the Chief of Naval Operations in Washington DC. A prior enlisted IT and Surface Warfare Officer, his last operational assignment was as the Combat Systems Information Officer aboard USS ESSEX (LHD 2) in San Diego, CA.

References

[1] The Hon. Michael J. Bayer, Mr. John M. B. O'Connor, Mr. Ronald S. Moultrie, Mr. William H. Swanson. Secretary of the Navy Cybersecurity Readiness Review (CSRR), March 2019. https://www.navy.mil/strategic/CyberSecurityReview.pdf

[2] Ibid

[3] Ibid

[4] Ibid

[5] Chief of Naval Operations, December 2018. Design for Maintaining Maritime Superiority, Version 2.0. https://www.navy.mil/navydata/people/cno/Richardson/Resource/Design_2.0.pdf. p. 3

[6] Wayne P. Hughes, 2000. *Fleet Tactics and Coastal Combat*. Annapolis, MD: Naval Institute Press.

[7] Bayer, et al., CSRR 2019, p. 12

[8] Security Magazine, Apr 24, 2019. "What's the Average Cost of an Insider Threat?" https://www.businesswire.com/news/home/20180424005342/en/Research-Ponemon-Institute-ObserveITReveals-Insider-Threat

[9] CNO, Design 2.0, p. 13

[10] Secretary of the Navy, 12 Mar 2019. Letter accompanying public release of the CSRR 2019. https://www.navy.mil/strategic/SECNAVCybersecurityLetter.pdf.

[11] Ibid.

Featured Image: U.S. 7TH FLEET AREA OF OPERATIONS (Oct. 16, 2015) Operations Specialist 1st Class Keith Tatum, from Americus, Georgia, stands watch in the Combat Information Center (CIC) aboard the guided-missile cruiser USS Normandy (CG 60) during an air-defense exercise as a part of the joint exercise Malabar 2015. Malabar is a continuing series of complex, high-end warfighting exercises conducted to advance multi-national maritime relationships and mutual security. Normandy is deployed to the U.S. 7th Fleet area of operations as part of a worldwide deployment. (U.S. Navy photo by Mass Communication Specialist 3rd Class Justin R. DiNiro/Released)

SHARE THIS:

Email Tumblr Print Facebook LinkedIn Twitter Reddit Pinterest

LIKE THIS:

Like

Be the first to like this.

Related

Initiative of the Subordinate: Dudley Knox and the Modern U.S. Navy
August 15, 2016
In "Book Review"

A Cyber Vulnerability Assessment of the U.S. Navy in the 21st Century
January 31, 2017
In "Capability Analysis"

History's Data for Tomorrow's Navy
April 25, 2017
In "History"

CYBER FEATURED IW NAVIFOR

3 THOUGHTS ON "NAVY CULTURE MUST BE ADAPTED TO FIT THE INFORMATION AGE"

John Griffin

JUNE 18, 2019 AT 8:00 AM

The Navy War College can help. Read this piece in Cyberdominance: https://www.cyberdominance.com/dominance/information-warfare-is-fleet-business/

Richard Mosier

JUNE 19, 2019 AT 2:22 PM

The fact that navy commanders view cyber security as someone else's problem can be addressed by formally making it their problem, with "career skin in the game" as a motivating factor. One might even envision snap inspections of commands to assess their cyber security readiness, or active probing by US "counter cyber" entities to identify weaknesses and vulnerabilities.

John Griffin

JUNE 20, 2019 AT 8:21 AM

Agree. We need to get after it in multiple vectors. Inspections, career competitiveness implications, etc., all help inject energy into the system now to shake up the inertia. Simultaneously, the most effective way to change a culture is through education and the early socialization opportunities.