The U.S. Navy's Evolving Cyber/Cybersecurity Story

Rear Admiral Nancy Norton

A BRIEF HISTORY OF NAVY CYBER

You can't pick up a newspaper or view a cable news program without hearing about cyber, whether cyberattacks, cyber defense, offensive cyber, cybersecurity, cyber threat, *cyber Pearl Harbor,* etc. You might think this issue just popped up the last few years. But all the armed services have been thinking about cyber for a number of years, in fact DEPSECDEF John Hamre originally used the term "cyber Pearl Harbor" in the 1990s, SECDEF Leon Panetta repeated it in 2012. The Navy in particular has been thinking about cyber for a long time.

The origins of the military's emphasis on cyber and cybersecurity can be traced back to at least 1996, when Joint Chiefs of Staff Chairman General John M. Shalikashvili, U.S. Army, released Joint Vision (JV) 2010. This seminal publication championed "Full Spectrum Dominance" as the "...key characteristic we seek for our Armed Forces in the 21st century."

JV 2010 stated, "The fusion of all source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations. Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive *picture* which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it."

Rear Admiral Nancy Norton serves as Director of Warfare Integration for Information Warfare. As an information professional, RDML Norton has served in information dominance billets at all levels, afloat and ashore. She commanded Naval Computer and Telecommunications Station Bahrain during Operation Iraqi Freedom. Rear Admiral Norton served as executive assistant to the Chief of Naval Operations from 2010-2012, and most recently as the director, Command, Control, Communications and Cyber Directorate, U.S. Pacific Command. RDML Norton is a native of Oregon and graduated from Portland State University with a Bachelor of Science in General Science. Norton earned a Master of Science in Computer Science from the Naval Post-graduate School and a Master of Arts in National Security and Strategic Studies from the Naval War College, where she was the President's Honor Graduate.

Cebrowski and Net-Centric Warfare

At the same time, the U.S. Navy moved full steam ahead into Information Age Warfare with its own approach, "Net-centric Warfare", which first appeared in 1995 in the Department of Navy's publication, "Copernicus: C4ISR for the 21st Century." The ideas of networking sensors, commanders, and shooters to flatten the hierarchy, reduce the operational pause, enhance precision, and increase speed of command were captured in this document. As a distinct concept, network-centric warfare appeared publicly in a 1998 US Naval Institute Proceedings article by Vice Admiral Arthur K. Cebrowski and John Garstka, and later in the book Network Centric Warfare: Developing and Leveraging Information Superiority by Alberts, Garstka and Stein published by the Command and Control Research Program (CCRP).

The introduction stated, "Network Centric Warfare is the best term developed to date to describe the way we will organize and fight in the Information Age. The Chief of Naval Operations, Admiral Jay Johnson, has called it "a fundamental shift from platform-centric warfare." We define NCW as increasing combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

NMCI

While the Navy was focusing on the warfighting aspects of cyber, Navy leaders also recognized the immense challenges in managing the ever-growing collection of disparate computer networks, which posed a massive security threat. With no enterprise-level oversight, individual commands could buy and install their own computer systems at will.

Local commands were left to manage the security of their systems. The answer to this problem was the Navy Marine Corps Intranet (NMCI), and its follow-on enterprise network services approach, Next Generation Enterprise Network (NGEN). Under the orders of Secretary of the Navy Gordon England, beginning in 1999, NMCI consolidated roughly 6,000 networks, some of which could not e-mail, let alone collaborate with each other, into a single integrated and secure IT environment.

In a 2004 speech, England noted that, "One of the most pressing areas that needed attention was security. It wasn't just that we weren't following our own rules; in many cases we weren't even aware of them."

Attacks and Threats

In the years following the standup of NMCI, the topics of cyber and cybersecurity surfaced occasionally, usually coincidental to some specific security incident, and not always connected to activity within Navy or DoD systems.

In 2008, Russia directed 'Zombie' infected computers around the world to barrage web sites in the country of Georgia, including the pages of the President, the Parliament, the Foreign Ministry, news agencies and banks, demonstrating that cyberattacks had moved beyond hackers or hactivists to the realm of international geopolitics.

The US military was also targeted that year. Operation Buckshot Yankee responded to an infection from inserting a USB flash drive into a laptop computer at United States Central Command. The flash drive was left in a base parking lot in the Middle East, infected by a foreign intelligence agency with malicious code that spread when the device was plugged in.

Network Centric Warfare is the best term developed to date to describe the way we will organize and fight in the Information Age.

In 2013, Mandiant Security Consulting Services released a report documenting evidence of cyber attacks by China's People's Liberation Army targeting 141 organizations in the United States and other countries as far back as 2006.

For the U.S. Navy, this series of eye-openers culminated with a major incident in 2013.

Vice Admiral Jan Tighe, Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet (FCC/C10F) talked about the incident in Congressional testimony on March 4, 2015:

"...we fought through an adversary intrusion into the Navy's unclassified network. Under a named operation, known as Operation Rolling Tide (ORT), U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber

Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cybersecurity posture and defensive operational capabilities."

For the U.S. Navy the intrusion mitigated through Operation Rolling Tide marked a significant *cyber awakening.*

Task Force Cyber Awakening

Navy leaders realized our inability to holistically understand, and command and control, its cybersecurity posture across the Navy, beyond just the corporate navy networks, to include combat and industrial control systems. The Navy also lacked a single enterprise authority to manage cybersecurity. These shortcomings manifested themselves in confirmed exploits and lost data, known vulnerabilities, limited cybersecurity situational awareness, and inadequate safeguards.

To gain that necessary perspective, Admiral Jonathan Greenert, Chief of Naval Operations and Sean Stackley, Assistant Secretary of the Navy for Research, Development and Acquisition, chartered Task Force Cyber Awakening (TFCA) in August of 2014.

TFCA was a year-long effort, led by the office of the Deputy Chief of Naval Operations for Information Warfare (N2/N6), under Vice Admiral Ted Branch. The goal was to baseline the cyber security of the Navy across all systems, afloat and ashore, and determine a way ahead to improve defenses. TFCA was tasked to deliver fundamental change to the Navy's organization, resourcing, acquisition and readiness by extending our cybersecurity apparatus beyond traditional IT to our combat systems, combat support and other information systems while aligning and strengthening authority and accountability.

TFCA formed four Task Groups (TG), each with representation from across the Navy.

- TG Capabilities reviewed cyber security actions and assessments already underway or recently completed to prioritize investments to ensure that Navy was taking the right steps in the near-term.
- TG CYBERSAFE constructed a program, modeled after the SUBSAFE program developed by the submarine community following the loss of USS Thresher in 1963. The CYBERSAFE program would apply to a hardened, very limited subset of components and processes and include rigorous technical standards, certification and auditing.
- TG Navy Cyber Security focused on evaluating current authorities, methods and resources required to best apply rigorous technical standards, certifications and assessments across the Navy.

- TG Technical used senior engineers from the Navy's systems commands to ensure that robust, common technical standards and authorities were put in place to drive cyber programs and systems.

TFCA prioritized protection efforts based on recommendations from industry, the cybersecurity community and stakeholders, then evaluated hundreds of funding requests for addressing vulnerabilities, with $300 million set aside in fiscal year 2016, and additional investment in the five year budget, to strengthen the Navy's defenses and improved awareness of its cybersecurity posture.

Navy Cybersecurity Division

In September 2015, the CNO established the Navy Cybersecurity Division on the headquarters staff (under Vice Adm. Branch's N2/N6 organization) to continue TFCA's transformation efforts. The new division oversees the Navy's approach to cybersecurity, developing strategy, ensuring compliance with cybersecurity policy, and advocating for cybersecurity requirements. The division will also evaluate and prioritize major investments and manage the CYBERSAFE program.

But the Navy cybersecurity effort is not just the responsibility of the Navy Cybersecurity Division. There are a number of other Navy organizations who are critical to the cybersecurity fight and who are making significant contributions to improving the Navy's defenses. They include:

- Navy Chief Information Officer: Establishes policy and guidance relating to IT.
- Fleet Cyber Command/U.S. 10th Fleet: Operates, maintains and defends Navy networks and conducts cyber operations.
- Information Forces Command: Organizes, mans, trains and equips the cybersecurity workforce.
- Systems Commands: Strengthen cybersecurity throughout the lifecycle of systems with the goal of "baking in" security from the beginning instead of "bolting it on" after systems are fielded.

As Vice Adm. Branch points out every chance he gets, "The cyber threat is real. This fight is ongoing even as we speak; right now Navy cyber warriors are defending against hackers, cyber-terrorist, and nation-state actors. Furthermore, every day the solutions I buy for the Navy as the DCNO for Information Warfare make our warfighting platforms, communications systems, and business systems more connected through cyberspace... and therefore a bigger target."

The Department of Defense alone experiences 41 million scans, probes and attacks per month.

CONCLUSION

With those last few statements, it is very clear. The Navy's focused effort has come a long way from the days when cyber was looked at as simply an emerging capability that we needed to exploit. Cyber is now a recognized operational domain, alongside the more traditional land, air, surface, subsurface, and space domains.

Within the Navy, cybersecurity is now considered an enduring mission. We have made it clear, in discussions, communications and training, that cybersecurity is now the responsibility of every commander and commanding officer. It is no longer just passed down to the computer professionals behind closed doors in the basement of the building or the lower decks of the ship. Cybersecurity demands an *all hands* effort.

It is very simple, whenever a Navy Sailor, civilian or contractor logs onto a Navy computer or connects to a Navy system, they are in the cyber battlespace.

We must stay in front of the ever-evolving cybersecurity challenges that face the Navy, the Department of Defense, and our great nation.

Now and in the foreseeable future, it is *all hands on deck.*