Naval Cyber Security:

The Desperate Necessity of Enhanced Information Dominance and Cyber Security for a New Era of Warfare.

Word Count:

2139

When technology advances, warfare advances. In the Information Age, the internet and cyber space are the newest battlegrounds for warfare and data is the newest weapon. Data determines decision-making and worldwide communication is the lifeblood our U.S Navy runs on to maintain its superiority in an ever changing, more connected world. The Lines of Effort outlined in, "A Design for Maintaining Maritime Superiority 2.0" aim to help increase our competitive advantage over our advisories and it is the prioritization of Cyber Security that can help the Navy achieve these goals.

The U.S Navy, as well as the United States Government as a whole, needs to recognize the importance of the Cyber Domain and how, when exploited, it can lead to catastrophic consequences. One example of the crippling power of a cyber-attack on infrastructure is a malware named, Petya/NotPeyta/Nyetya/Goldeneye, which infected multiple countries in 2017 and as Wired.com reported, "Researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank." (Wired.com, 1)

With the ability to cripple an entire country by controlling and wreaking havoc on its infrastructure, the need for a Cyber Security Defense Forces should be paramount. In reference to Design 2.0, the Competition-Conflict Spectrum, Information Warfare is broad in its abilities to be peaceful and lethal at the *same* time. Networks and technology connect every system and every platform the Navy owns. A focus and improvement in Cyber Security allows us to attack, defend, and counter all at the same time, giving the Navy a massive competitive advantage.

The same way the Navy has established and fortified itself around the world, enabling us to, at any moment, strike and defend against hostile acts is the same way we need to treat Cyber Space. With our reliance on networks, technology, and intergraded weapon systems, losing the ability to communicate with ourselves, our allies, or even with each other garrotes the Navy and effectively blinds operations that may not cause immediate damage, but as is the case in warfare, delays and disruptions of battle rhythms could mean the difference between victory and defeat.

How does Cyber Security help achieve LOE Blue? For one Cyber Security can improve our protection of weapon systems, which right now may not be as secure as we think. The F-35 is a cutting edge weapon, yet it's been proven to be vulnerable to targeted hacking. In 2018, a two-person test team was able to, "gain initial access to a weapon system and one day to gain full control of the system they were testing." (GAO,2,pg22) The Government Accountability Office (GAO), reported, "Mission-critical cyber vulnerabilities in nearly all weapon systems that were under development… potentially susceptible to compromise." (GAO, 2, pg 21) This is only going to increase with our dependency of interconnectivity to the world around us.

Along with lacking Cyber Security Defensive Posture, there is another concern with Cyber Security in terms of Offensive Posture as well. In order to fulfill LOE Blue, we need more Cyber Commanders to help reinforce decision-making and develop, "Cyber Force Units," to increase lethality in the Cyber domain. We as a Navy have the ability to strike and defend anytime and anywhere in the world at a moment's notice, but on the Cyber Battlefield, we need

to present that same strength. A common practice that strengthens our abilities, fosters cooperation with allies and displays our Naval Power are the Joint War Games. If we had a focus on, “Cyber War Games,” we can take the same simulated warfare environment to Cyber Space and improve both our defensive and offensive capabilities in Cyber. If LOE Blue wants to Strengthen Naval Power, we must be as powerful in Cyber as we are maritime.

With LOE Green wanting to achieve high velocity outcomes, Cyber Security can meet this requirement. All the new platforms and weapon systems we develop will no doubt enhance our arsenal and further our competitive margins, there lies an echo with LOE Blue, how can we protect these assets not only from direct Cyber Intrusion, but also from keeping our technology from leaking in to the wrong hands? Contractors are one of the biggest targets for Chinese Cyber Operations which, as LOE Green states, is where most of the new platforms and weapons are going to be developed from. In June of 2018, the Washington Posted reported a Chinese hack that stole massive amounts of data concerning submarine warfare, an area of the Chinese Military that we still have an advantage over.

In the report, “614 gigabytes of material relating to a closely held project known as Sea Dragon, as well as signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit’s electronic warfare library.” (WP, 3, internet link) While this incident is major, it increasingly emphasizes the need for increased focus of Cyber Security, not only for the DoD/Navy, but for our Contractors as well. By having policy dedicated to Cyber Security Protocols for our awarded contracts, we help to ensure our High Velocity Outcomes stay safe, secure, and provide the advantage we need over our adversaries.

Cyber Security can greatly enhance our outcomes with protection of assets and future technology, but while the CNO wants to modernize our current enterprise of networks, we should be going beyond modernization and instead, be the industry leaders. If we want to retake our competitive advantage over our adversaries, it isn’t enough to simply meet standards, we must go above and beyond, and we need to lead. Dedicating research to advanced, internetworking systems that don’t rely on the Internet is one direction we can take towards securing our data and technology. An increase in Military, ethical hacking teams benefits the Navy by finding exploits before they happen and also saves the Navy time and money on patching exploits instead of dealing with the damage the comes from malicious attacks. High Velocity Outcomes are achieved when the focus can be on mission success, not from cyber damage control or bound by technological crippling.

LOE Gold, in terms of Cyber Security, is the biggest security concern but also a massive opportunity for Cyber Security. Beginning with the security concern, LOE Gold has an objective of making MyNavy Portal accessible without a CAC with a mobile platform. Technological convenience begets a give a take relationship with security. The easier a system or process is to access, the more vulnerable it becomes. The example I use for this massive security risk is accessing these records on unsecured public networks like, say, at Starbucks or any other café. Because a network can’t be trusted, there runs a high risk of unscrupulous hackers waiting for a suspected military member to access MNP and finding out that sailors personal information,

records, etc. Simply put, when it comes to accessing records, payroll, and all the other services MNP offers, ease of mobile access is too risky.

Kabir Chibber published an article on October 19, 2014 for Quartz about how hackers can learn about your life from a coffee shop Wi-Fi network. From the article Kabir learned of an ethical hacker named Wouter Slotboom,

"Slotboom created a fake Wi-Fi network at a cafe with an understandable name ("Starbucks" rather than "BT201238"), which makes more people likely to jump on to his network. He gets 20 devices in a short space of time, and is able to look at the traffic coming to and from their phones, laptops, and tablets and exploit bugs if the devices have outdated operating systems." (Quartz, 4)

While the majority of LOE Gold relates to sailors family and education/training, a huge opportunity for cyber security enhancement is the chance for sailors to be able to explore opportunities and training for different rates. A perfect example of this is the skills of a CTM versus that of an IT. A CTM, as stated by Navy COOL, performs installation, configuration, diagnosis, and repair of state-of the-art electronic, computer, and network hardware and software systems. (Navy COOL PDF, 5) Then with the rate of IT, they, "Perform core and specialty functions of network administration; install applications and peripherals, troubleshoot user problems, and provide assistance with the use of computer hardware and software including printers, word-processors, electronic mail systems, and operating systems; conduct system backups and restores; utilize knowledge of database management systems to maintain, administer, test, and implement computer databases." (Navy COOL PDF, 6)

When we allow for modernization or, "Cross Rate" training, we can combine the hardware centric CTM with the networking/database management skills of an IT to create a truly powerful sailor who can not only design, install, and build a system, but can update, troubleshoot, and manage the system all together, eliminating the need to have multiple teams of people to specialize is one aspect of a certain system. This type of hybrid training allows for a huge push in Cyber Security training by exposing all sailors with the skills needed to either support or take part in Cyber Security. An CTT with some basic knowledge of an IT/CTN can not only provided missile defense, but can actively monitor their system for foreign intrusion to stay 100% ready at all times.

The last LOE, LOE Purple, echoes the points previously made about the connectivity of our world and how much we depend on networking and communication to ensure success. Updated or new policies regarding Cyber Security are essential in maintaining a secure networking environment for all levels of access, from unclassified networks to TS/SCI networks. Along with our need for Cyber Security enhancement within our own military and government, our allies can also benefit from an enhanced Cyber Security standard.

A perfect example of this is with the recent controversy of Huawei Telecommunications Company as a national security risk because of unmanageable components. From another article from the Washington Post, "International partners took a "skeptical" stance on U.S. claims that Huawei's components present such a threat to cybersecurity and national security that it cannot

be managed, said several participants in the meetings." (WAPO, 7) With an updated, industry leading focus on Cyber Security, the US would have a stronger influence over the control of technology use from foreign countries like China, who have been known users of Cyber Espionage. By becoming leaders of Cyber Security, we stand to make our alliances stronger by protecting allied countries and ultimately helping the US Government secure joint operations and allied networks who could potentially be an unsecured source of US targeted attacks.

The 5th point of LOE Purple is another reason for increased Cyber Security for the Navy. Academia and non-government research institutions are absolutely critical sources of knowledge and technological advancements that not only help further the Navy's power, but help American society as a whole. Unfortunately, Universities and research institutions are a coveted target for foreign hackers, from a curious individual to state sponsored hacking force. Shannon Liao, a reporter for The Verge published an article titled, "Chinese Hackers Reportedly Targeted 27 Universities for Military Secrets," where it described how universities were targeted by spear phishing as a means to infect university systems with malware. Many of which have ties to contractors or the Navy itself.

When Admiral Richardson stated in his conclusion that, "The margins of victory are razor thin, but decisive," and that, "We must pick up the pace and deny them," means that we need a refocused, higher priority to Cyber Security and Information Warfare. LOE Blue represents a path towards Cyber Dominance in a new battlefield that will ultimately determine the next major conflict. If we are to continue to be the world's most lethal, maritime fighting force, we must have equal or greater dominance in Cyber Space. LOE Green is achieved through Cyber Security by protecting our new platforms and weapon systems. In order to lead the charge in Cyber Warfare, it isn't enough be modern, but to push advancement to keep a strong lead over our adversaries. LOE Gold provides ease of administration, but simultaneously potentiates a security concern. Risking sailor PII in a hyper connected world is just as dangerous as open sourcing weapon systems. Lastly, LOE Purple must be enhanced with Cyber Security in order to secure our research, develop technological advances, and protect our technological lead against or advisories.

The world is becoming interconnected and more technical at an exponential rate. Our land, air, and sea power are the most powerful the world has ever known and it's critical that we, as the US Navy, bring that superiority in to Cyber Space not only as a means of quickly and efficiently ending conflict without violent means, but also as our duty to protect American interests and secure a free, open cyber environment for our nation and our allies.

SOURCES AND CITATIONS:

1. Newman, Lily Hay. "The Biggest Cyber Security Disasters of 2017 So Far." *Www.wired.com*, 2017, www.wired.com/story/2017-biggest-hacks-so-far/.
2. United States Government Accountability Office. "WEAPON SYSTEMS CYBERSECURITY DOD Just Beginning to Grapple with Scale of Vulnerabilities." *www.gao.gov*, 2018, https://www.gao.gov/assets/700/694913.pdf
3. Ellen Nakashima and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." *www.washingtonpost.com*, 2018 https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.1c732047e61f
4. Kabir Chibber. "What a Hacker Can Learn About Your Life from the Coffee Shop's Wi-Fi Network." *www.qz.com*, 2014, https://qz.com/283461/what-a-hacker-can-learn-about-your-life-from-the-coffee-shops-wi-fi-network/
5. US Navy. "CTM – Cryptologic Technician (Maintenance)." *www.cool.navy.mil*, 2019 https://www.cool.navy.mil/usn/enlisted/rating_info_cards/ctm.pdf
6. US Navy. "IT – Information Systems Technician." *www.cool.navy.mil*, 2019 https://www.cool.navy.mil/usn/enlisted/rating_info_cards/it.pdf
7. Ellen Nakashima and Brian Fung. "U.S. Allies Differ on Difficulty of Containing Huawei Security Threat." *www.washingtonpost.com*, 2019 https://www.washingtonpost.com/technology/2019/03/06/us-allies-are-skeptical-trump-administrations-huawei-argument/?noredirect=on&utm_term=.8c5c173085f3
8. Shannon Liao. "Chinese Hackers Reportedly Targeted 27 Universities for Military Secrets." *www.theverge.com*, 2019 https://www.theverge.com/2019/3/5/18251836/chinese-hackers-us-servers-universities-military-secrets-cybersecurity