Andrew Sherbinin

Cybersecurity in the Navy

The May 7th pipeline hack demonstrated that America's vital infrastructure can be disabled by domestic groups that can potentially be backed by any government on the planet with adequate resources. Likewise, the dependency we have on systems that can be crippled by foreign powers challenges how we should think about cybersecurity in the current data era. However, only on the surface are most groups for-profit. State actors are more than capable of providing malicious groups with unlimited resources to disrupt American infrastructure and acquire valuable data on classified information.

The infrastructure and supply chains that supply America's Navy and Marine Corps can be vulnerable to attacks by state-backed groups, and these can be China, Russia, or Iran. In the 21st century, data is currency. To the USMC and Navy, this data lies in the form of encrypted communication and classified information. An important part of the various challenges that cybersecurity specialists tackle is securing all these various forms of data at their source and in transit.

Like every other teenager out there, I'm building some sort of data profile on the internet, in cyberspace. The music I listen to, the texts I send, and the photos I post are what led me to learn about cybersecurity in the first place. The problem with just understanding what you're posting online is that it doesn't matter to a hacker. If you use the internet for anything at all, you are susceptible to cybercrime. At its core, government stability is at stake. The same tech that the United States uses to fight against cyber threats is falling into the hands of foreign actors, which in a Cyber Arms Race, can bring a country to its knees. As many ships as the Navy acquires, it should equally invest its resources in protecting all the valuable data it sends out, as whoever invests the most wins. Similar to how the U.S. outspent the Soviet Union in the Cold War with nukes, and its industrial complex, likewise cybersecurity should have the same focus in gaining an advantage.

The Cybersecurity People

The "Cyber Dudes" out there battling threats in real time, assessing threats, and analyzing cyberspace are the primary people equipped to identify the virtual issues that the Navy faces. Threat intelligence analysts and security architects are only the bedrock of what goes into building a secure cyberspace, as dozens of components go into securing the Navy's data. Dr. Waleed Barnawi is one of those people out there that serve to design the offensive and defensive capabilities that protect against these threats. More importantly, "Cyber Nurses" or engineers like Barnawi help shape how data sets and systems can be protected against the threats that you normally wouldn't see outside of the military. Work that people like him do benefits not only the government but normal everyday people.

Part of my interests that led me to cybersecurity was from learning about people that have changed the world behind the scenes. Barnawi helped me realize that there are careers out there that support people making world changing decisions, and that's what cybersecurity can be.

The Future of Information

In 1923 General Billy Mitchel correctly predicted the next course for naval doctrine for the next one hundred years. He understood that carriers and naval aviation were the future of warfare nearly twenty years before they truly took their current course whenever Japan attacked Pearl Harbor, exactly how Billy Mitchel envisioned it. Dr. Waleed Barnawi envisioned that twenty years from now we're going to see an entirely new shift in how cyberspace is integrated within the military. We can already see the

forefront of how machines like the F-35 can “talk” with other systems. However in the future, we’re going to see engineering and communication linked much more substantially in everyday life with implanted sensors that can detect cancer cells before they really materialize and new tools to advance quality of life for humans. On the other line though you’re going to see a transformation in how cybersecurity is linked in a physical standpoint when it comes to protecting the Navy, Marine Corps, and everyday people.

Whenever Billy Mitchel predicted the attack on Pearl Harbor he was shunned and condemned by nearly everybody in the War Department. However, he knew what was coming, and similarly, cybersecurity specialists across the country see what is coming as the May 7th pipeline hack was foreseen. The Navy can shape and adapt in the face of adversity and crisis, just like it did after Pearl Harbor. However, this time it shouldn’t wait until another catastrophe strikes it to finally adapt to a changing climate.