Ethan Ho

What makes a war, well, a war? Does a war have to be fought with mighty weapons of steel and explosives? Or with thousands of soldiers charging across the battlefield? Is war limited to bombs, gunfire, and bloodshed on battlefields? The reality is, however surprisingly, that the answer is no. Attacks can come from anywhere enabled by human technology, and cyberspace is no exception. This is why cybersecurity is an essential part of the Navy and Marine Corps, as war is increasingly becoming more technology-involved. As our world is changing, the weapons we use to fight wars are changing as well.

As technology changes and the number of cyberattacks increase, who keeps our country equipped for the future of defense and war? They are people like Dr. Waleed Barnawi, the “Cyber Dude'' at the Office of Naval Systems. Dr. Barnawi thinks of cyberspace as a big hotel with many rooms needing the right locks to keep the world safe. By using different kinds of encryption and having regular “cyber checkups'' to make sure equipment is secure, people like Dr. Barnawi are keeping our country safe. Dr. Barnawi’s career and work inspires me because he is able to use skills in engineering, computer science, and research to defend the country. This is something that I would like to do as a career, to be able to use my skills to help advance a greater cause. I not only aim to acquire an undergraduate education, but also am inspired to obtain a graduate degree to research the problems of the future.

To see how important the cybersecurity research of the Navy and Marine Corps is, let us imagine the year 2040. In less than twenty years, humans have grown so much more reliant on computers that a mass cyberattack on a country could completely destroy the economy and even threaten the lives of many. And as the reliance on technology has grown, so has the need for cybersecurity. Remember back in 2021 when that pipeline was hacked with ransomware, costing $4.4 billion in ransom payments? People had no gasoline for their vehicles and there were long lines at every gas station. That won’t happen again. New backup systems, using fully homomorphic encryption to allow for easy updating of the backups, have been set up in all U.S. corporations and federal offices. Remember back in 2017 when the infamous WannaCry worm infected hundreds of thousands of computers using a protocol that was more than 35 years old at the time? That won’t happen again either. New vulnerability-scanning software on each of our computers, powered by artificial intelligence, patch vulnerabilities at the same time exploitation is detected. The whole system is open-source and decentralized so that no one entity controls the vulnerability scanning network. But where did these technologies originate? Unsurprisingly, they came from Navy and Marine Corps research. Before private companies took up the technologies, the Navy had been doing research on the encryption technologies that allowed for efficient backups. The Marine Corps had been developing ways to automate “cyber checkups” for military devices, which became the AI vulnerability patchers of today.

Now back to 2021. What’s the moral of this illustration? It’s how many of the technologies that impact our daily lives today have come from the Navy and other branches of the armed forces, and new technologies currently being developed there will continue to impact our lives in coming years. Our military is working hard to prevent the wars of the future and it is not with bombs or masses of steel. So the next time you see a new technology coming up in the latest tech startups, consider the Navy and Marine Corps. Maybe it was developed there!