# Jonathan He

Cybersecurity is a growing field of interest as millions of devices connected to the cyber realm every day are vulnerable to being hacked or injected with malware. Just this June, the Colonial Pipeline, the largest US fuel pipeline, was hacked. This event alone caused gas prices to soar and cars lining back blocks away, waiting for a refuel. Luckily, these horrifying situations could be addressed and solved through a team of cybersecurity experts working to fix hardware and software vulnerabilities before resorting to paying millions of dollars as ransom. Although the pipeline incident primarily affected the economy, it could be fatal if these cyber attacks were focused on military units such as the Navy and Marine Corps. A simple botnet injected into the Navy's Naval Operational Supply System could lead to starvation as soldiers and sailors who are unable to access their food and water that are locked away in smart storage appliances onboard newer ships. Meanwhile, there could also be more detrimental attacks including those that could cause docking systems at ports to malfunction, which will likely cost people's lives onboard the ship or on the port, and also millions of dollars spent to repair the docks. Although these scenarios may sound fictional or unthinkable, their occurrences may happen one day unless a greater leap is made to secure these critical systems. This is precisely the reason why cybersecurity interests me and why I chose this topic to write about for this application. The work done in cybersecurity is essential to prevent the costly incidents, in both lives and money, from ever occurring as well as to ensure safety and national security. Without a doubt, development in cybersecurity is ongoing and each step we make in advancing cybersecurity means one additional costly error avoided and another step closer to complete safety.

Indisputably, the scientist that inspires me in the videos the most would be Dr. Waleed Barnawi. Although I am immensely active within the cybersecurity area already and have done some research in this area, the video displaying the interview with Dr. Waleed Barnawi opened up doors that never occurred to me. This video made me realize and aware of the shortage of cybersecurity professionals. It is clear that the ratio between vulnerable devices out in the world and cybersecurity professionals is not even close to a 10000:1 ratio. Just the Navy and Marine Corps themselves include millions of devices, varying from technologies inside mission control to technologies onboard the ships. This encompasses so many different types of devices and technologies and it would be difficult for cybersecurity professionals to ensure that every single device is securely configured and protected. However, as Dr. Waleed Barnawi mentions, there are so many different pathways that could lead someone into a cyber-related career. Every contribution, no matter how minimal, to the cybersecurity area could lead to favorable results. All it takes is for us to keep learning and try our best to minimize the vulnerabilities and risks associated with connected devices, software, and systems in order to make the world a better and safer place.

Development in technology is rapidly growing each day. In fact, in just a few years, Mars travel and exploration may become a reality according to NASA's strategic plan. In 15 to 20 years, our world will become more connected through rapidly-changing intelligent technologies and devices. We will see significant increases in automation and optimization on Navy ships at sea and in bases. Interconnected devices, intelligent software,  automated processes, and fast processing of data will provide tremendous opportunities to help the Navy and Marine Corps become more efficient and effective in operation and in their fight to win against opponents. In the meantime, artificial intelligence and big data technologies will be widely leveraged by cybersecurity professionals to monitor billions of connected IoT sensors and devices in real-time, detect malicious or abnormal behavior, and take proactive approaches to secure the ships and prevent hacking incidents from happening. Faster computers such as quantum computers will become available by 2040 to make the detection of malicious behavior from massive amounts of data easier and quicker. Hackers may use quantum computers to attack vulnerable devices on navy ships as well. Future cybersecurity professionals will need to develop quantum-safe security countermeasures, techniques, and algorithms to battle against these new attacks before they happen.