Ava McLaughlin

CYSE 200T

March 6, 2025

Captain O’Donovan Guest Speaker

BLUF: Captain Brett O'Donovan, the Commanding Officer of Naval Computer and Telecommunications Master Station Atlantic, shared incredibly valuable insights during Tuesday’s class. The three topics that particularly grabbed my attention were CYBERCOM, NCTAMS LANT, and the CIA triad.

CYBERCOM

COCOMS are the Unified Combatant Commands of the U.S. military, responsible for overseeing military operations in specific regions of the world. There are Geographic Combatant Commands (GCCs) and Functional Combatant Commands (FCCs), the former based on geographic location and the latter on specific missions. Captain O’Donovan specifically works under CYBERCOM, an FCC, which focuses on cyber operations and defense. Directly under CYBERCOM is the Fleet Cyber Command, of which the tenth fleet is the Navy’s portion. He mentions CTFs 1010, 1020, 1040, 1050, and 1060, which oversee networking (DoDIN Ops), defensive cyber, and signal intelligence (alongside the National Security Agency). Captain O’Donovan’s CYBERCOM explanation was helpful because it explained and encouraged further research on how cybersecurity practices are applied globally.

NCTAMS LANT

Under CTF 1010 are NCTAMS (Naval Computer and Telecommunications Area Master Station) and NCTS' (Naval Computer and Telecommunications Station). Captain O'Donovan is the commanding officer of NCTAMS Atlantic, based in Norfolk, Virginia. He shows a helpful map of the scope of NCTAMS alongside a list of operations, which made the information easier to take in. He notes some of their operations include messaging (sending messages when normal IP internet traffic isn't available), VTC hubs, the fleet network operations center, and NC3 (communicating nuclear command and control functions either offensively or defensively). This discussion was very interesting and displayed just how large and intricate the Cybersecurity field is.

CIA Triad

Captain O'Donovan provides great examples of how the CIA triad is applied across the Cybersecurity field. He mentions he mainly deals with the accessibility portion, often getting frustrated end user calls because of multi-factor authentication. This shows how balancing accessibility with cyber defense is often complicated, and Cybersecurity is a team-oriented field. Further along in his discussion, he ties availability to transport, in which he discusses the flow of information through satellites, teleports, and other devices. Availability can be disrupted by jamming a satellite, for example, preventing communications and navigation. For confidentiality, they use very heavy encryption that is NSA-certified. Regarding integrity, transect is used which ensures the bits are the same between destinations, preventing someone from changing the data in between. Hearing how the CIA triad is applied in specialized operations furthers my understanding of it and displays its significance throughout the Cybersecurity field.

Conclusion

Captain O’Donovan is very experienced, and his insights were very valuable for my understanding of cybersecurity, primarily in the U.S. military. It is a broad field that spans global operations like CYBERCOM to local operations such as NCTAMS LANT, including many interconnected subsections that must collaborate to protect the military, government, civilians, and other nations. The CIA triad is also very prevalent, demonstrating that although cybersecurity is a vast field, it is built on core principles that every cybersecurity enthusiast should be familiar with; the NIST framework serves as another example.