Christopher Sicle

12/3/2024

CYSE 270

Navy Cyberwarfare Doctrine: The Danger of Malware

The Department of the Navy Cyberwarfare Doctrine is a comprehensive plan for how the US Navy will address cyberspace in the future with the goal of Cyberspace superiority. The strategy emphasizes “Defending Enterprise IT, Data, and Networks,” which indicates a significant threat: Malware. The Secretary of the Navy warns that malware seriously threatens national defense. This attack can disrupt weapon systems, steal sensitive data, or damage critical infrastructure. It is crucial to protect American interests, as these malware attacks threaten both military and civilian cyber domains. The Navy protects itself against these dangers, highlighting the situation's urgency. The strategy highlights the need to detect and respond to cyber incidents but raises questions about how to implement it. It does not clearly explain how to deal with new malware threats, such as polymorphic or AI-driven malware. This is concerning because our adversaries are continuing to evolve in cyberspace. We can only hope that information is “need to know” on how they plan to attack and defend against it. The Doctrines' focus is also limited, as they highlight state-sponsored threats such as those from Russia and China. While we study Cybersecurity, we know these are not the only threats out there, especially given the growing threat of cyber terrorism. In regards to training, which I believe is paramount to the success of the cybersecurity doctrine, it seems detailed what they want to accomplish by hitting the entry-level knowledge with the basics of cybersecurity training, making it a robust and expansive objective. However, it does not outline how it will adjust and adapt to every changing tactic that advisories.

In conclusion, while the Navy's strategy effectively identifies malware as a central cyber threat, it must expand its view to address its dynamic, decentralized nature. I agree with the Navy's training plan to improve overall cyber awareness. The Navy can only safeguard its cyber operations against the evolving landscape of malicious software it may employ by combining defenses with a global strategy.

References

Department of the Navy. (2023, November). *Cyber Strategy*. https://media.defense.gov/2023/Nov/21/2003345095/-1/-1/0/DEPARTMENT%20OF%20THE%20NAVY%20CYBER%20STRATEGY.PDF