Self-Reflection on

MST 684 – Cyber Threat

by

Alejandro F. Sosa

This Unclassified paper was submitted to the faculty of the National Intelligence University in partial fulfillment of the requirements for the Master of Science and Technology Intelligence Portfolio.

October 2024

Introduction

The Cyber Threat course equipped me with the knowledge and analytical tools to assess cyber threats from state and non-state actors. This course introduced a comprehensive framework for understanding how cyber-attacks are planned, executed, and mitigated. By exploring threat actors, methodologies, and strategies, I gained practical insights into the complexity of modern cyber warfare and the importance of developing adaptive intelligence approaches. This reflection will focus on the key learning areas: assessing threat actors, understanding attack methodologies, and applying threat models to real-world scenarios. This course is also where I became extremely interested in Quantum Information Science as an overall topic. The artifact I chose for my portfolio is the essay I wrote on Quantum threats and use cases.

Evaluating Cyber Threat Actors and Capabilities

One of the most valuable aspects of this course was the deep dive into the capabilities, motivations, and strategies of various cyber threat actors. I learned how different nation-states, terrorist organizations, hacktivists, and cybercriminals use cyberspace to achieve their objectives. For example, we compared how state actors like Russia, China, and North Korea focus on espionage and political influence, while non-state actors, such as ransomware groups, seek financial gain through exploitation and extortion. This analysis gave me a more nuanced understanding of how threat actors align their activities with broader strategic goals, such as disrupting rival economies or manipulating public opinion.

Additionally, the course provided insight into how the cyber capabilities of different actors vary based on resources, technical expertise, and access to tools. I found it particularly interesting to explore how some non-state actors purchase malware-as-a-service or collaborate with state sponsors, blurring the line between state and criminal activities. These discussions

underscored the importance of attribution and the difficulties involved in accurately identifying the source of cyber-attacks.

Understanding Attack Methodologies and Exploitation Techniques

The course also focused on the methodologies cyber threat actors use to carry out attacks. We analyzed the stages of a cyber-attack, from reconnaissance and initial compromise to escalation, exploitation, and data exfiltration. This framework helped me understand how attackers gain access to systems, escalate privileges, and evade detection. By studying these processes in detail, I developed a greater appreciation for the sophistication of modern cyber-attacks and the importance of proactive threat monitoring.

Another important concept was the identification of attack vectors, such as phishing campaigns, zero-day exploits, and supply chain vulnerabilities. We discussed how threat actors target specific systems or individuals to gain entry and how they leverage human error or weak security protocols to succeed. These lessons reinforced the importance of both technical and behavioral defenses in mitigating cyber threats.

Applying Threat Models to Real-World Scenarios

Our group project analyzed real-world cyber incidents, such as ransomware attacks and espionage campaigns. My group chose to analyze the Triton malware attack, an attack on a chemical facility that leveraged vulnerabilities in the company's networks and allowed access to the facility's operational control systems. These activities enhanced my teamwork and problem-solving skills and demonstrated the importance of intelligence sharing and collaboration in the cyber domain. This was actually one of the more organized and responsive groups I have worked with. We set project milestones, brainstormed options outside of class using Google

collaboration tools, and integrated our project sections well before the deadline. I use many of the strategies that we used to collaborate as a group when leading other group projects.

Conclusion

Overall, the Cyber Threat course has helped me to develop a comprehensive understanding of the actors, methodologies, and strategies shaping today's cyber landscape. It equipped me with practical tools to assess cyber-attacks, evaluate vulnerabilities, and develop threat models that align with national security and organizational goals. I now have a deeper appreciation of the complexity of cyber operations and the importance of collaboration between intelligence agencies, private sector partners, and policymakers. Moving forward, the insights and skills I gained from this course will be invaluable in my pursuit of a career in cyber intelligence, where adaptability, critical thinking, and proactive analysis are essential for success.