Mitigations for Cyber Operations Below the Level of Armed Conflict

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Abhinav Dinesh is a Software Engineering Analyst for CACI International Inc. He is an undergraduate student pursuing a Bachelor of Science studying Management Information Systems and Business Analytics as a student participant in the PREP program at George Mason University's Costello College of Business.

Maya Stephens is a Cybersecurity Engineering Intern with Serco Inc. She is a graduating undergraduate student earning her B.S. in Business with a Concentration in Management Information Systems as a student participating in the PREP program at George Mason University's Costello College of Business.

Mobeen Raja is a graduating undergraduate student pursuing a B.S. in Business with a Concentration in both Management Information Systems and Business Analytics at George Mason University's Costello College of Business as a student participant in the PREP program at George Mason University's Costello College of Business.

----- ***Industry Participant / Mentor*** -----

Alison ward
Analyst
US Cyber Command

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty, Dean's Teaching Fellow, & FWI Corporate Partner Faculty Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

In today's connected world, technology has always been an aspect of our lives that never leaves. As the world gets more connected, technology is heavily reliant in sectors like communication and commerce making collaboration across borders easier. However, this large reliance on technology makes us vulnerable to exposing critical infrastructure and subject to cyber attacks from across the world. Since the first modern cyber attack, cyber espionage has evolved as a consistent threat where state-sponsored cyber attackers or Advanced Persistent Threats (APTs) use complex cyber attack tactics to cripple and manipulate infrastructure. Cyber Attacks have reached a level of concern so drastic that governments deem it as one of the largest threats to national security resulting in the creation of Cyber Institutions to fight these attacks. In addition, this paper will also explain the definition of "level of armed conflict" as it pertains to cyber attacks and the best practices to mitigate these attacks.

Business Challenge

What actions are our adversaries taking to conduct cyber operations against the United States and its allies below the level of armed conflict?

Activities Done to Address the Business Challenge

We suggest these mitigations to address the issues of APT tactics used against the US:

Strong Identity and Access Management	• Least Privilege Principle
	  ○ Only allow users with the privileges that they absolutely need
	  ○ Limit the need to move laterally through systems
	  ○ This prevents credential dumping
	• Multi-Factor Authentication (MFA)
	  ○ In the event an account is stolen, MFA is a second line of defense

Signature based behavioral analytics	• Gives preemptive indicators of a possible cyber attack by monitoring digital signature of user

Endpoint Detection and Response	• Microsegmentation
	  ○ Blocks cross-zone access with the use of PowerShell commands
	• No implicit trust
	  ○ Every login is treated the same and implements the same processes for logins

Zero Trust Architecture	• Insider Risk Management
	  ○ Prevents insider data theft and other exfiltration activities
	  ○ Mitigates Potential Risky behavior form users

	• Data Loss Prevention
	  ○ Guards against unauthorized data use
	  ○ Helps Classify Data
	  ○ Encrypt files with classification labels

Cyber Hygiene and Employee awareness training	• Recognize unusual behavior • Act ethically and promptly when it comes to identifying cyber attacks

Conclusion

With the rapid changes in technology and the reliance it comes with, individuals and governments need to understand the threat of cyber attackers and the methods they take to perform their objectives. Foreign threat actors have an advantage of not needing "boots on the ground" to wreak havoc and chaos, but with an active plan of mitigation to possible threat actors, especially APT's, We can have a grasp on the safety of our systems and our national security. Protecting our Nation's information with Zero-trust, employee awareness, strong identity and access management and the other mitigation strategies mentioned will give us the best chance at protecting the Confidentiality, Integrity and Authenticity of our data. With these strategies we can effectively protect our nation from cyber operations below the level of armed conflict.

PREP Student Reflection

Participating in the PREP program, along with working on this project with US Cyber Command, was a very rewarding and insightful experience for our team. Throughout the semester, we had opportunities to research everyday cyber problems and find solutions to solve them. This experience allowed us to implement what we learned in our MIS classes and apply it to real situations, an opportunity to go beyond the usual classroom routine.

Meeting with Ali each week allowed us to stay focused and grounded in the real-world context of our task. She challenged our research, asked us to rethink certain angles, and always had suggestions that helped us get closer to our goals. Ali helped us gain a better understanding of how the United States Cyber Command responds to threat actors. Also, Meeting with Professor Ngac weekly helped us refine our work for Ali, as he helped us navigate the academic expectations while keeping the project on track.

Working on a project tied to a real government organization was a different experience, as it added a layer of realness and motivation. We came out of this with a better sense of how cybersecurity works in the real world, not just in a classroom, and we gained more confidence in applying our research and analysis skills in that environment. Overall, this experience made us think differently about teamwork, responsibility, and the actual impact of the work we do.