**Lab Assignment 02:**

**Cyber Warfare – DoD Cyber Strategy**

Micah Flack

Department of Computer Science, Dakota State University

CSC 840 DT1: Cyber Operations I

Dr. Michael Ham

September 9, 2022

**Summary**

Since the beginning of COVID19, cybercrime in general has risen 600% (“2022 Cyber Security Statistics Trends & Data,” n.d.). To combat this, the Department of Defense (DoD) has proposed five strategies:

* Build a More Lethal Force
* Compete and Deter in Cyberspace
* Strengthen Alliances and Attract New Partnerships
* Reform the Department
* Cultivate Talent

All of which, has been coined repeatably in the news as a “defense forward” approach. Meaning, the DoD intends to respond to future cyber threats by building up their response capabilities for military action before or absent any armed conflict. This is a stark contrast to their philosophies in past administrations since they have historically preferred reactive responses over the now suggested preemptive ones (*Not The Cyber Deterrence the United States Wants | Council on Foreign Relations*, n.d.). As the number of daily cyber-attacks against critical infrastructure continues to climb with each year, the DoD has recognized the need to overhaul the existing culture and internal responses to cyber warfare.

**Strategic Competitor**

North Korea is home to several advanced persistent threats (APTs), namely APT38, Operation WizardOpium, Wassonite, Kimsuky, APT37, Darkhotel, and Covellite (*APTMAP - Advanced Persistent Threat Map*, n.d.). But there is another more infamous group from there as well. The Lazarus Group, known to be the operators behind the infamous Sony hack in November of 2014 (Fagerland, n.d.). They have also been attributed with attacks as far back as Dozer in 2009, Koredos in 2011, Joongang Illbo attack in 2012, and DarkSeoul and KorHigh in 2013. Recently, the group was identified behind several attacks against the Department of Energy last week (*North Korean Lazarus Hackers Take Aim at U.S. Energy Providers*, n.d.).

Researchers at Cisco Talos found that the group was targeting exposed VMWare Horizon servers, using publicly known vulnerabilities, from February to July 2022. Then pivoting with their own custom malware such as “Vsingle” (*VSingle Malware That Obtains C2 Server Information from GitHub*, n.d.), “YamaBot” (*YamaBot Malware Used by Lazarus*, n.d.), and another remote access trojan called “MagicRat” which is used to further collect more information from the victim’s devices (*North Korean Hackers Deploying New MagicRAT Malware in Targeted Campaigns*, n.d.). What makes this especially noteworthy is that VMWare Horizon requires higher privileges to run. Assuming a malicious operator has an exploit to gain that access, they then have the necessary elevated controls to modify registry keys and disable protective services like Windows Defender or launch WMIC and PowerShell commands for the following stages.

**5-Year Response**

Given the timeline we previously illustrated for the Lazarus Group, it is hard to believe that the United States as a nation will have any chances to slack their cybersecurity responses without grave consequences. For instance, in 2021 alone there were 66 novel zero-day attacks. In 2020, there were nearly half as many of those attacks, at only 38 (“2022 Cyber Security Statistics Trends & Data,” n.d.). All of which are actively being leveraged against critical assets.

Among those zero-days identified in 2021, there were several new vulnerabilities documented for Schneider Electric’s industrial control systems (ICS) (*Zero Day Vulnerabilities in Industrial Control Systems Highlight the Challenges of Securing Critical Infrastructure*, 2021). Which is one of the more frightening areas to watch for vulnerability development, because we unknowingly rely on these systems at every waking moment. These are devices called PLCs and HMI used to control industrial factory equipment and machines; if a hacker were to gain malicious access to one of them, it could be fatal to the workers or completely shut down important services (*2 Critical Vulnerabilities in Rockwell PLC Used Worldwide Could Shutdown Industries for Days If Exploited*, n.d.; Constantin, 2022).

**Strategic Approach**

Arguably, each of the approaches carries their own significance and a greater impact towards the overall security posture and readiness of the nation. However, the “Reform the Department” approach is likely to be the most important because it will determine the DoD’s ability to follow through with the other four parts of the strategic approach. Like a security awareness campaign within a company, the factors behind the department changing successfully are bound to be more similar than not.  
Of which there are several key factors to watch for, as follows:

1. Is the department able to identify motivations and communicate well?
2. Are the awareness materials engaging and not rely on fear invocations?
3. Does leadership understand the importance and meaning of cyber awareness?
4. Is the funding available to make changes as needed?
5. Are there any cultural differences that would affect perception of the awareness campaign or reception towards preferred behavioral changes? (Bada et al., n.d.)

Whether or not the DoD leadership is able to directly address these issues will determine the overall success with the department reformation, especially with their allies and partners.

# References

*2 critical vulnerabilities in Rockwell PLC used worldwide could shutdown industries for days if exploited*. (n.d.). Retrieved September 9, 2022, from https://www.securitynewspaper.com/2022/04/01/2-critical-vulnerabilities-in-rockwell-plc-used-worldwide-could-shutdown-industries-for-days-if-exploited/

2022 Cyber Security Statistics Trends & Data. (n.d.). *PurpleSec*. Retrieved September 9, 2022, from https://purplesec.us/resources/cyber-security-statistics/

*APTMAP - Advanced Persistent Threat Map*. (n.d.). Retrieved September 9, 2022, from https://andreacristaldi.github.io/APTmap/#45

Bada, M., Sasse, A. M., & Nurse, J. R. C. (n.d.). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* 11.

Constantin, L. (2022, August 16). *“Evil PLC Attack” weaponizes PLCs to infect engineering workstations*. CSO Online. https://www.csoonline.com/article/3669914/evil-plc-attack-weaponizes-plcs-to-infect-engineering-workstations.html

Fagerland, S. (n.d.). *THE HISTORY OF THE DARKSEOUL GROUP AND THE SONY INTRUSION MALWARE DESTOVER*. 78.

*North Korean Hackers Deploying New MagicRAT Malware in Targeted Campaigns*. (n.d.). The Hacker News. Retrieved September 9, 2022, from https://thehackernews.com/2022/09/north-korean-hackers-spotted-using-new.html

*North Korean Lazarus hackers take aim at U.S. energy providers*. (n.d.). BleepingComputer. Retrieved September 9, 2022, from https://www.bleepingcomputer.com/news/security/north-korean-lazarus-hackers-take-aim-at-us-energy-providers/

*Not The Cyber Deterrence the United States Wants | Council on Foreign Relations*. (n.d.). Retrieved September 9, 2022, from https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants

*VSingle malware that obtains C2 server information from GitHub*. (n.d.). JPCERT/CC Eyes. Retrieved September 9, 2022, from https://blogs.jpcert.or.jp/en/2022/07/vsingle.html

*YamaBot Malware Used by Lazarus*. (n.d.). JPCERT/CC Eyes. Retrieved September 9, 2022, from https://blogs.jpcert.or.jp/en/2022/07/yamabot.html

*Zero Day Vulnerabilities in Industrial Control Systems Highlight the Challenges of Securing Critical Infrastructure*. (2021, July 13). Tenable®. https://www.tenable.com/blog/zero-day-vulnerabilities-in-industrial-control-systems-highlight-the-challenges-of-securing