TOPIC: The potential threat of cybersecurity networks and cyberspace being militarized.

School of Cybersecurity – Old Dominion University

Your Major: Cybersecurity

Your Name: Marcus Sowers

Your ID: 01179669

ABSTRACT

Cybersecurity networks and the cyberspace has expanded over the last few decades. In these last few years, war has been an on-going and common issue around the world whether it's over different reasons, like power or land. Internet militarization has already been used as a tactic to ensure state and national security, while keeping civilians protected from potential cyber threats within the networks. With cybersecurity and cyber networks steadily expanding on the daily, potential attacks within the network also increases. In this paper I will go into detail and discuss into detail why cybersecurity networks and cyberspace are at a potential risk of being militarized.

Key Words: Cyberspace, Cyber Attacks, Cyber Warfare,

INTRODUCTION

Cybernetworks and cyberspace is continuously involving and expanded in today's world. Everyone is beginning to gain access to these networks, making it available and more common for everyone to understand and take advantage of this luxury. These certain advantages could be potentially a good or bad thing. In this research paper, it will discuss the potential threat of these networks and cyberspace of being militarized. It will go into great detail of what these networks and cyberspace is, what exactly are the threats from cyber-attacks and warfare, and the gains of militarized networks.

CYBERSPACE

Cyberspace is the global internet environment in which communication and shared information over computer networks occurs. Everyone that has access to the internet will also have access to

communication and information through all these computer networks. With everyone allowed to have access to this, it could be a potential issue if a certain person or country wanted to take advantage of it. In a scholarly journal used for this research paper, it is stated that the "incentives for moderation are built into its cooperatively constructed infrastructure, and these incentives grow stronger as more economic and administrative functionality moves online" (Duncan B. Hollis). This should open everyone up to the idea that they are always potential risk as everything is beginning to move online and is advancing to technology. This extremely large computer network connecting computers globally is great for instant reliable communication and information transactions. Even though it has its pros, it is also understandable why people must consider its cons. The cyberspace is at huge risk of being potentially attacked and possibly militarized if used correctly. Multiple countries and certain individuals are beginning to understand these networks and take advantage of the opportunities to execute attacks and data breaches. With this being stated, the next point that will be discussed in this research paper is the understanding of cyberattacks and warfare.

CYBER ATTACKS

A scientist named Willis Ware delivered a conference paper that stated, "the dangers of resource-shared computing, especially for military and defense systems, arguing that deliberate attempts to penetrate such computer systems must be anticipated" (William Marrin). This conference paper and statement gives great understanding why there will always be a risk of potential attacks and possible misuse of militarized cyberspace. The specific paper by Mr. Ware discussed directly "on the threat of deliberate penetration, including active in filtration of systems and passive subversion tapping communication lines" (William Marrin). Different countries could possibly execute these acts of cyberattacks creating an opportunity to upgrade their country and military power.

CYBER WARFARE

In one reference used for this research paper, a guy named Richard A. Clarke stated, "Cyberwarfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network. Or any other activity affecting a computer system, in which the purpose is to add, alter or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls" (William Merrin). This

also creates an understanding that cyber technology is at risk because of cyberattacks and disruption within computer systems for military purposes.

Cyber/Military Test and Gain

Military interest has been increasing, just like the rate of computer networks and the cyberspace. One source found in the references launched a cyberwar exercise called 'Eligible Receiver', and this exercise tasked a "NSA 'red team' to infiltrate DoD networks using only commercially available technologies. Intrusion turned out to be 'absurdly easy'. The two-week test was over within four days, as the NSA team penetrated the entire defense establishment network, leaving markers to demonstrate their access and even interfering with communications: 'They intercepted and altered communications, sent false emails, deleted files and reformatted hard-drives'. Eligible Receiver was another proof-of-concept of both the possibilities of penetration and of actual disruption and damage" (William Marrin). This information is a great base for understanding and recognizing that even though one might think a military network or cyberspace is secured and protected, there is always a possible way that the information or data is at serious risks from attacks and non-authorized personnel. Another study has also proven that "the complexity of cognitive work associated with human-technological interaction with multiple interdependent, interconnected and networked environments is compounded, as these human and technological agents consequently bring their own assets and goals (e.g., informational, social, physical, cyber) into the operating and decision-making space" (Øyvind Jøsok). This proves that regardless of rules and ethical guidelines that must be followed, there will always be a small percentage of countries or individuals that may not follow for personal gains.

CONCLUSION

In conclusion, this research paper went over in great detail and understanding of why cybersecurity networks and cyberspace are at a potential risk of being militarized. It highlighted on of what these cyber networks and the cyberspace is, what exactly are the threats from cyber-attacks and warfare, and the possible gains of militarized networks. It provided a cyber exercise that was launched that expressed the gains of militarized networks and space, while also explaining why it is at risk within this world. These results and finding should make everyone open their eyes to potential military threat, while creating more of an understanding on what is at potentially at risk.

REFERENCES

Merrin, William. Digital War. 1st ed. Milton: Routledge, 2018. Web.

Campbell, Peter. "Generals in Cyberspace: Military Insights for Defending Cyberspace." Orbis (Philadelphia) 62.2 (2018): 262-77. Web.

Jøsok, Øyvind, Benjamin J Knox, Kirsi Helkala, Ricardo G Lugo, Stefan Sütterlin, and Paul Ward. "Exploring the Hybrid Space." Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience (2016): 178-88. Web.

Haataja, Samuli. Cyber Attacks and International Law on the Use of Force [e-book] the Turn to Information Ethics (2019). Web.

Patel, S. (2019). A Grim Gap: Cybersecurity of Level 1 Field Devices. Power, 163(2), 31–33. Web.

Deibert, R. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. Millennium (03058298), 32(3), 501–530. Web.