Cyberterrorism Across the Globe

Alexander O. Kotzian

School of Cybersecurity, Old Dominion University

CYSE 426: Cyber War

Dr. Saltuk B. Karahan

April 14, 2024

Abstract

The integration of technology within the daily lives of citizens has allowed for a communication system not seen at any point in time throughout our history as a species. It has created a convenient and physically safe environment to interact with other people across the globe as well as the means to produce virtual communities that directly interact with our physical communities. Additionally technology and by extension internet access has allowed for the increased effectiveness of physical infrastructure of organizations. These benefits come at a significant downside, they are vulnerable to attacks by individuals that could be anywhere in the world. The most detrimental attacks result in a significant disruption in infrastructure processing. The most pressing matter in recent years has been hackers and hacker groups that virtually attack infrastructure as a means to conduct terroristic acts. These cyber terrorists are becoming more effective and broad reaching, hampering some of the most powerful nations in the cyber security field. In this paper I intend to describe some of the most impactful cyber attacks on nations, some cyberterrorist groups, and some unforeseen connections between cyberterrorists and national governments.

Keywords: Terrorism, cyberterrorism, technology, cybersecurity, security.

Introduction

The evolution of technology has brought about a vast web of communication that has the potential to interact with anybody or any entity on the globe. This has developed into a vast social environment that allows for the creation of groups of individuals with shared goals that can interact with others across the globe. The social structure that has come as a result of the sudden connection of these social groups is the rise of extremist groups. Some of these groups have further consolidated their ideology into that of cyber action against nations as a means of terrorism. These terrorist groups typically attack high-level corporations or government infrastructure. In certain situations governments may have assistance in a foreign cyberattack from these cyberterrorist groups.

What is a Cyberattack?

In order to understand cyberterrorists and how they conduct acts of terror we must understand the most impactful act they commit, which is a cyberattack. A cyberattack in its most basic form "is a deliberate computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system, or damages or steals the information it contains" (Kenney 2015). This allows us to understand that a cyberattack is a direct attack from one device to another and therefore has the most potential of occurrence.

Cyberterrorist attacks

Considering our baseline understanding of a cyberattack, some examples of cyberterrorist attacks should help highlight the impact of cyber terrorist groups and the impacts they have through their acts. The North Korean cyberterrorist group by the name of 'Lazarus group' had conducted the cyber attack known as WannaCry. This WannaCry ransomware attack produced a worm that "spread to more than 200,000 computers in over 150 countries. Notable victims included FedEx, Honda, Nissan, and the UK's National Health Service." (Cloudflare 2021). This is one example of a cyberterrorist group with ties to its national government. Additionally in 2018 a member of this cyber terrorist group was charged for "his involvement in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware and, and the extensive loss of data, money and other resources" (Office of Public Affairs 2018). Particularly in the situation regarding the cyber terrorist group known as Lazarus group, we see the goal of the cyberattack in its simplicity to terrorize the nations and companies it affects. This is highlighted in the disruption it had on the United Kingdom's National Health Service, this had the potential to cost lives as it extremely disrupted the resource management of hospitals affected by WannaCry. The WannaCry ransomware was

seemingly unhinged in its limitations as it affected any computer exposed to it. The Lazarus Group also conducted a cyber terrorist attack as a response to the movie *The Interview*. Due to their ties to the North Korean National Government, this was meant to intimidate the publisher behind the movie from giving access to the movie to the public.

A allegedly russian-backed cyberterrorist group by the name of Fancy Bear has conducted a cyberattack that consistently affects Russia's decision to conduct continuous warfare and could have potentially helped spark the Russo-Ukrainian war. Fancy Bear developed an X-Agent which was an application that was constantly updated, but "enabled artillery forces to more rapidly process targeting data for the soviet-era D-30 Howitzer employed by Ukrainian artillery forces reducing targeting time from minutes to under 15 seconds" (CrowdStrike Global Intelligence Team pg 2. 2016.). This had major implications for the Crimean Crisis when Russia annexed Crimea in 2014. This provides context as to their effectiveness. Additionally this cyberattack is significant because it is a passive attack that assists in the destruction of life through the means of conventional warfare.

Another Russian based cyber terrorist group by the name of DarkSide intruded on and locked the function of the Colonial Pipeline network behind a ransomware attack. The results of the attack were that the Colonial Pipeline paid the price the group was asking for, setting a precedent for future ransomware attacks on critical infrastructure businesses. "The hacker group, on the ransom note, demanded a payment of 4.4 million dollars to release the network" (Beerman, Berent, Falter, Bhunia 2023).

Moving on to the Chinese based cyber terrorist group labeled by the United States as APT31, we have a court case regarding the charging of seven PRC nationals with "conspiracy to commit computer intrusions and conspiracy to commit wire fraud for their involvement in a

PRC-based hacking group that spent approximately 14 years targeting U.S. and foreign critics, businesses, and political officials in furtherance of the PRC's economic espionage and foreign intelligence objectives (Office of Public Affairs 2024). This furthers the common reality that many cyber terrorist groups are backed whether it be financially, technologically, or politically by national governments or agencies as a means to further the influence that nation has over the international community. This group in particular has conducted itself in a fashion that directly correlates to the politics of the PRC. This cyber terrorist group is used as a tool by the PRC to conduct itself in a way that intimidates and disrupts anything that may be considered an adversary by the PRC. Additionally it furthers the goals of the PRC throughout the global community.

Anonymous

The most influential hacker group in the global community is simply known as Anonymous. The anonymous group is a decentralized community that incorporates a large number of people with the perceived goal of exposing digital information and secrets that they believe should be available to the public. This group's structure makes it extremely unique in its function. The structure of this group provides a means for gray hat hackers to collaborate with each other to perform large hacks and events. What makes this group unique in their comparison to the previously discussed groups is that they are not backed by a nation in particular. Therefore their goals are based purely on their ideological beliefs. This group is notorious for their ability to conduct large-scale public information dumps as well as calls to action. These work so effectively because they present themselves as a political group. Due to their presences as a political group they are able to hoax in politically similar individuals through their attacks. A movement they were heavily involved in particularly represented the ideals of left-wing

populists. This movement was known as Occupy Wall Street. Anonymous's involvement in this was that it heavily bombarded social media systems with the movement's message. Anonymous "announced plans to mobilize 20,000 people in lower Manhattan" during the events of Occupy Wall Street (Captain 2011). This plan provides a connotation of an organized movement meant to interject within the Occupy Wall Street movement and further the goals of Anonymous.

Anonymous's unorganized approach to cyberattacks has allowed for them to be described as the primary suspect in cyberattacks members of theirs would perform. This has provided a more negative attitude to the hacker group throughout the course of its existence, in addition to the attacks that it is the legitimate perpetrator of. This cyber terrorist organization is by far the most internationally involved due to its scale. Its origins are most likely within the United States due to its increased involvement in United States politics and economics in comparison to other nations. This is considerably unique in comparison to the nation-backed cyber terrorist groups. The intentions behind this group's actions are to create a political message and discourse that progresses to a goal, while the nation-backed cyber terrorist groups primarily intimidate and disrupt infrastructure. Anonymous additionally is non-discriminatory, while the nation-backed groups only target adversaries of their nations.

Conclusion

Throughout my research I have discovered that a majority of large scale cyber terrorist groups are backed by nations, whether it be through the means of funding, technology, or political support. The three nations discussed in this paper have provided a unique use for the cyber terrorist groups that they sponsor. North Korea's Lazarus Group has primarily been used to sow chaos and destruction to nations across the globe, as well as target imagery that is a negative portrayal of their government. Similarly China's cyber terrorist group designated APT31 is primarily used to conduct large-scale intimidation of adversaries of the PRC, this includes nations, individuals, and companies alike. Russia's Fancy Bear cyber terrorist group provides a collaborative relationship with Russian conventional forces to provide information that is strategic and vital to a war that has the intention of conquest. These nation-backed cyber terrorist groups collaborate with their respective governments to provide the means to a goal that the government wishes to achieve. In essence these cyber terrorist groups are simply a tool to the government. The most well-known and unique cyber terrorist group known as Anonymous houses a few stark distinctions to the other cyber terrorist groups discussed. Anonymous's goal is to provide a political message and garner increasingly more followers for their movement. The way they do this is by interjecting their own message into other movements that are occurring that may be beneficial to them such as the Occupy Wall Street movement. Additionally Anonymous conducts non-discriminatory cyber attacks that are meant to further their political message. However each of these groups are furthering their link to their governments or consolidating more power to their cause as time progresses. These groups are increasing their presence on a global scale. Therefore we must stay alert and proactive in our defense against these adversaries.

References

Kenney, Michael Cyber-Terrorism in a Post-Stuxnet World, Orbis, Volume 59, Issue 1, 2015, Pages 111-128, ISSN 0030-4387, https://doi.org/10.1016/j.orbis.2014.11.009 or https://www.sciencedirect.com/science/article/pii/S0030438714000787

What was the WannaCry ransomware attack? | cloudflare. Cloudflare. (2021). https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Office of Public Affairs. (2018, September 6). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. *North Korean Hacking Team Responsible for Global WannaCry 2.0 Ransomware, Destructive Cyberattack on Sony Pictures, Central Bank Cybertheft in Bangladesh, and Other Malicious Activities*. Retrieved from https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Crowdstrike. (2016, December 22). Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. Voice of America News. https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

J. Beerman, D. Berent, Z. Falter and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India, 2023, pp. 8-15, doi: 10.1109/CCGridW59191.2023.00017. or

https://ieeexplore.ieee.org/abstract/document/10181159?casa_token=8BM38YaAeiEAAAAA:GDHBRoTGDDem7ME4M_GuMZj1ziC6YjqPdmv90N_tx4Bi0hXoSJByTD2rHDlXsGodgnnNgzwZEg

Office of Public Affairs. (2024, March 25). *Defendants Operated as Part of the APT31 Hacking Group in Support of China's Ministry of State Security's Transnational Repression, Economic Espionage and Foreign Intelligence Objectives.* Retrieved from https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

Captain, S. (2011, October 18). *The real role of anonymous in Occupy Wall Street*. Fact Company. https://www.fastcompany.com/1788397/real-role-anonymous-occupy-wall-street

Word Count: 2045