Siobhan Dunn, Julia Fontana, Chiyoung Lii, Dennis Timmons

IST 623  Assignment 2

Cyber war & cyber terror

# Table of Contents

1. Introduction
2. Differences between cyberWAR and cyberTERROR
3. Cyberterror (ISIS)
4. Recruiting
5. Proliferating Propaganda
6. United States
   1. Cyberwar High Profile Targets
   2. Defending against cyberwar attacks
   3. 2016 Elections
7. International
   1. NotPetya
      1. History
      2. Purpose and Method of Operation
      3. Damage done by attack
   2. Iran 2010: Stuxnet
      1. History
      2. Purpose and Method of Operation
      3. Notable aspects of Stuxnet
8. Conclusion

# **CYBERWAR & CYBERTERRORISM**

# Introduction

# The words cyberwar and cyberterrorism are often used interchangeably and while many may think these two words mean the same thing, they have very different meanings in the information technology, military, and security industries. Because the words “cyber”, “cyberspace”, “cybercriminals”, and “terrorism” all have different definitions depending on the national government or governing agency, there are no standard definitions for the terms cyberwar and cyberterrorism. However, generally speaking, the term cyberwar refers to attacks initiated by one state government or entity over cyberspace being telecommunication or information systems that typically targets other state or national governments. Common goals of cyberwar attacks are to obtain government intelligence, disrupt military operations, or manipulate political influence. On the other hand, cyberterrorism generally refers to attacks that are initiated over cyberspace by violent extremist groups whose goals are to incite violent acts, proliferate propaganda, spread extremist ideology, and recruit members. Marsili, 2019, states that the Federal Bureau of Investigation defines cyberterrorism as “[any] premeditated, politically motivated attack against information, computer systems or computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents.” Contrarily to cyberwar, a significant portion of cyberterrorist activity occurs over the public internet in the forms of recruiting and distributing propaganda.

# In the following pages we will briefly discuss how ISIS uses the Internet to recruit members and spread ideology. We will also take a look at the United States’ defense policies and techniques to combat cyberwar, possible high profile cyberwar targets within the US, and the involvement of Russia influencing the 2016 US Presidential Election. Finally, we will end the discussion by taking an international view of cyberwar by examining several well-known case studies of cyberwar attacks outside of the United States.

# CYBERTERRORISM: *Ideology, Propaganda, & Recruitment*

# The exponential growth of the Internet, and more specifically the use of social media, over the last 15 years has created an environment where information can spread and be shared with millions of people almost instantaneously. Furthermore, the dark web enables users to share information and communicate in a space that is unregulated, uncensored, and anonymous. Realizing the potential to mass communicate ideology and distribute propaganda to attract potential members, terrorist groups such as ISIS shifted their recruiting strategies online.

# ISIS (the Islamic State of Iraq and Syria) originated is 2003 as a byproduct of the Iraq Invasion by the United States. In 2011, civil unrest and war in Syria opened a gateway for ISIS to claim a large amount of territory and establish a strong foothold by occupying major cities in the northern provinces of Syria and Iraq. The violent extremist group is most notoriously known for their ideologies that involve creating a singular unified Islamic state governed by Sharia law. Sharia law is a religious law derived from the Quran that advocates for the implementation of “…laws based on anti-liberal, backward, intolerant, misogynist interpretations [of the Quran] and establishing a caliphate [a unified Islamic state] by any means including the use of violence and terrorism…” and to create “…a social order that restricts personal freedoms, enforces patriarchy and imposes rigid gender-based norms…” (Mahood & Rane, 2017).

# The decline of ISIS began in July of 2017 when Iraqi Armed forces were able to liberate the city of Mosul which served as the ISIS stronghold in northern Iraq and forcing ISIS to flee to Syria. However, ISIS took another devastating blow when Syrian armed forces liberated the city of Aleppo, further shrinking the ISIS controlled territory in northern Iraq and Syria. ISIS control over the region continued to dissipate and the final blow occurred in October 2019 when a US Joint Special Operations Command conducted a raid to capture the ISIS leader, Abu Bakr al-Bagdadhi, who instead took his life by suicide bombing.

# From 2011 until their precipitous decline in 2017, ISIS established themselves as the most violent and most feared Islamic extremist group in the world. They successfully executed and claimed dozens of attacks all over the world ranging from London to Germany and even claiming responsibility for several shootings in the United States. ISIS was able to persuade thousands of people, Muslim and non-Muslim alike, into abandoning their families and joining the caliphate. They were able to accomplish this by building an elaborate recruitment network online where they could expose potential targets to extreme Islamic ideologies and propaganda depicting fantasized versions of life as an ISIS soldier.

# Although many adult Muslims joined ISIS for political and historical reasons, the primary targets for ISIS recruiters were young Muslims typically in their teens to early twenties. ISIS recruiters not only attracted young Muslims in the Middle East but also individuals in the younger Muslim populations of Europe and the United States who felt marginalized by the societies they lived in. Many younger Muslims living in Europe and the US felt that they were not fully accepted by traditional Muslims or by the western society they lived in. The yearning for acceptance and identity created an opportunity for ISIS recruiters to promote radical ideas. Muslims who have been victims of discrimination and marginalization in Western cultures were coaxed by ISIS anecdotes of an Islamic utopia or *Ummah* were all Muslims lived in a singular unified Islamic society that provided purpose and brotherhood. (Mahood & Rane, 2017).

# The primary danger of cyber-recruitment is its ability to quickly expose large online communities to a considerable amount of engaging, multimedia content (Scanlon & Gerber, 2014). Once engaged, recruiters initiate the process of radicalization by introducing narratives to manipulate and influence the target’s perception and point of view. In a study that analyzed the ISIS propaganda magazine Dabiq, Mahood & Rane, 2017, were able to identify the three most popular narratives, or interrelated and sequentially complex stories, that ISIS propaganda and recruiters use to first attract and then radicalize members. The top three narratives are:

# 1) The Crusaders

# 2) Jahiliyya

# 3) Hypocrites

# The Crusaders narrative appeared the most often in the study of ISIS propaganda recruitment. The narrative refers to the infidel invaders who occupy Muslims lands and must be repelled. ISIS uses this narrative to politically justify the creation of a sovereign and independent Islamic state. The second narrative that ISIS uses is the concept of Jahiliyya. Jahiliyya refers to a society or state characterized by the ignorance of God’s will, injustice, and vice. Jahiliyya is accompanied with the ISIS ideologies of implementing a society structure governed by Sharia law and that all societies in existence that do not abide by Sharia law are unjust, immoral, unholy, and must be destroyed. Jahiliyya demands the destruction of heretical Western cultures who do not adhere to Sharia law and the authority of Allah. According to ISIS ideology, true Muslims will never be safe unless the world is unified under a singular caliphate. The third most popular narrative used by ISIS recruiters is the narrative of the hypocrites. The hypocrites refers to all persons and populations around the globe who profess to be Muslim but secretly seek to undermine the Islamic state. Muslims who live in western cultures, adhere to western laws, and do not adopt the values of Sharia law and customs are not considered true Muslims by ISIS. Muslims living in the West are considered hypocrites who support western laws and policies that oppress true Muslims living in the Middle East. Western Muslims are further encouraged to abandon all social and family ties with those who do not obey ISIS’s laws and join their true brothers in the Islamic state. By using the hypocrite narrative “ISIS is attempting to delegitimize all interpretations of Islam other than its own and discredit the diversity of religious thought and interpretations within Islam, past and present.” (Mahood & Rane, 2017.)

# All three narratives share a common theme: US versus THEM. The crusader narrative shares the idea that the goals of Western societies are to undermine and oppress the Muslim world. Jahiliyya says that the only societies that should exist are ones governed by Sharia law and graced by Allah himself while also advocating violence and the destruction of Western civilization. Finally, the hypocrite narrative eliminates alternative interpretations of the Quran and declares that only true Muslims are those who live in the Islamic state. These narratives were powerful tools used by ISIS recruiters to radicalize and indoctrinate young Muslims. Due to the growing concern of cyberterrorism and cyber-recruitment, researchers and social media companies have enacted policies that detect and eliminate violent extremist content online. Early trials of anti-cyberterrorist software has shown “…that automatic violent extremist recruitment detection is a feasible goal…” and “...potential terrorist recruitment events…can be efficiently compiled into leads for current investigations or used as evidence to open new terrorism-related investigations.” (Scanlon & Gerber, 2014) The implementation of anti-cyberterrorism software in addition to the toppling of ISIS’s entire organization starting in 2017 has resulted in an abrupt decrease in cyber-recruitment efforts.

# Cyberwar: High Profile Targets

While it is easy to think of cyberwar and cyber terror as distant and occuring in foreign countries, the United States is involved and impacted by these as well. One popular and high profile target for cyberwar crimes in the United States and abroad are power grids. Countries can impose significant damage on each other by implementing code that disrupts or completely takes down access to power. The United States compromised Russia’s power grid in 2018 as a warning to President Putin. This was approved by the sector of the Pentagon that focuses on cyberwar and online attacks (Perlroth, 2019) The Department of Homeland Security and FBI believe that Russia has implemented malware in the United States as well that could significantly disrupt American power, gas, oil and water lines. (Perlroth, 2019) While neither side has activated their codes, these breaches have the potential to create widespread damages should the cyberwar between Russia and the United States ever become more aggressive.

# Defending Against Cyber Warfare (United States)

Cyber warfare takes forms that may not be as obvious, or in formats traditionally associated with war at all. In the digital age, technologies exist at our fingertips that can completely redefine our lives and the lives of others; such technologies exist for national governments as well, to utilize to the advantage of their countries.

Additionally, it is happening between nations in ways that may not be realized by civilians, and defense against these attacks is happening as well. In the United States, Department of Defense (DOD) Secretary Dr. Mark T. Esper has stated that the cyberspace has emerged as a choice domain for nations that wish to engage in war against the United States, and that in response, defense teams have worked towards hardening networks to better protect against such attacks (Garamone, 2019). Though, despite their efforts to implement and improve cyber training, their focus on defense will not be enough. As Esper disclosed, likely in response to harsh critics, the United States is beginning to implement an offensive strategy for securing the nation’s cyberspace and is investing heavily in increasing their offensive cyber skillset.

An extremely unique example of cyber warfare, arguably, existed between Russia and the United States during the 2016 Presidential Election in the US. Realized for the first time, a foreign nation leveraged information communication technologies (ICTs) via social media platforms, primarily Facebook, to manipulate a presidential election in the United States. Defense Secretary Esper believes the DOD has an important role to play in defending the American public from these varied attempts to manipulate elections that may continue to occur as we saw during the 2016 election cycle (Garamone, 2019). Only time will tell what evolved cyber warfare defense will look like in the United States as cyber trends continually change much faster than the government.

2016 US Presidential Election

During the 2016 Election Cycle in the United States, evidence has surfaced to support the claim that Russia attempted to interfere with the election, beginning as early as 2014. While the exact motive of the interference is uncertain, some believe it was a result of Vladimir Putin’s distaste for Hillary Clinton, the Democratic candidate in the election. As the Mueller Report disclosed, it is believed that actors backed by Russia worked to spread propaganda against Clinton across social media platforms, seemingly in efforts to sway public opinion of United States voters, as Clinton polled higher. Much of this work was done by actors posing to be American political activists, through organizations like the Internet Research Agency and, most famously, Cambridge Analytica.

Cambridge Analytica was a UK-based political consulting firm that collected data from Facebook users about their political affiliations through a personality app developed by Professor Aleksandr Kogan of Cambridge University. Kogan later went to work for the campaign of President Donald Trump. Through this personality quiz application, third-party Cambridge Analytica was able to gather information pertaining to users of the app as well as these users’ friends’. It was later discovered that this information collected was accessed from Russia.

Interestingly, the scandal of Cambridge Analytica called to action Mark Zuckerberg, who testified before Congress about Facebook’s role in the permission of data collection by third-party applications. The case of Cambridge Analytica has sparked a much larger conversation and public concern over user privacy when using social media platforms, as well as bringing to the forefront the need to regulate them.

# Case Study: NotPetya

There have been numerous cyberattacks around the world that prove that cyberwar is an ongoing concern. A large and notable example of a cyberattack is NotPetya, a malware created and distributed by Russia. The NotPetya attack was the result of an ongoing war between Ukraine and Russia. (Greenberg, 2018) A group of Russian military hackers who were known as Sandworm hacked into Ukranian government organizations and Ukranian companies including railway companies, media outlets, and power companies. The attacks to the power companies happened in the middle of winter two years in a row, which caused the greatest amount of harm from the widespread power outages that occurred. (Greenberg, 2018) After these preliminary attacks, Sandworm began it’s main attack in 2017. They targeted a company called Linkos Group, which is similar to TurboTax in America. Sandstorm compromised Linkos Group’s update server and used it to push the NotPetya malware to the thousands of computers across Ukraine that it had backdoor access to through the server. They had control of this server for many months without the company knowing and without releasing the malware right away, waiting for the right time to do the most damage. (Greenberg, 2018)

## Purpose and Method of Operation

NotPetya has two exploits. The first is called EternalBlue, which was actually created by the United States but leaked in 2017. This section of the attack uses a vulnerability in a Windows protocol that allows hackers to run their own code on any unpatched machines. The second is called Mimikatz, which was created by a French security researcher in 2011. Mimikatz is able to pull passwords out of a computer’s RAM and use those passwords to hack into any other machine that uses the same credentials. While Microsoft did release a patch to prevent EternalBlue from being successful, if there was even a single computer on the network that was not patched NotPetya could get to that computer and then Mimikatz allowed NotPetya to be spread across all the other computers even if they were patched. NotPetya moved at incredibly fast speeds to infect entire networks. It took down one of the largest banks in Ukraine in only 45 seconds, and fully infected a major transit hub in 16 seconds. (Greenberg, 2018)

After a computer or network was infected with NotPetya, the hackers would demand large sums of money in Bitcoin from the companies or individuals who were promised that their computers would then return to normal. (Banerjea, 2018) However, the computers were irreversibly encrypted so it was not possible to revert a computer back after it had been compromised so the payments were made in vain. (Greenberg, 2018) This was particularly concerning as it was estimated that at least 10% of all computers in Ukraine were infected with NotPetya during this attack, which essentially shut down many companies and the government. (Greenberg, 2018)

## Impact

Although Russia’s intent was to attack Ukraine with NotPetya malware as part of their cyberwar, the effects were even more far reaching. The malware ended up being spread to many multinational companies including Merck, FedEx and Maersk. (Banerjea, 2018) Maersk is a European company with 80,000 employees that was notably impacted by this attack. Within half an hour of the first computer being taken over by the ransomware, the entire company was compromised and infected by the malicious software so that no computers on their network could be used. (Greenberg, 2018) NotPetya even unintentionally ended up back in Russia, where it infected the state oil company Rosneft. (Banerjea, 2018)

This attack resulted in approximately $10 billion in damages worldwide, which is arguably the most destructive cybercrime in history. (Banerjea, 2018) Pharmaceutical company Merck suffered about $870,000,000 in damages, FedEx had $400,000,000 losses and Maersk had $300,000,000, just to name a few of the highly impacted companies who were not the intended victims. (Greenberg, 2018)

# (Microsoft, 2017)

# Case Study: Stuxnet

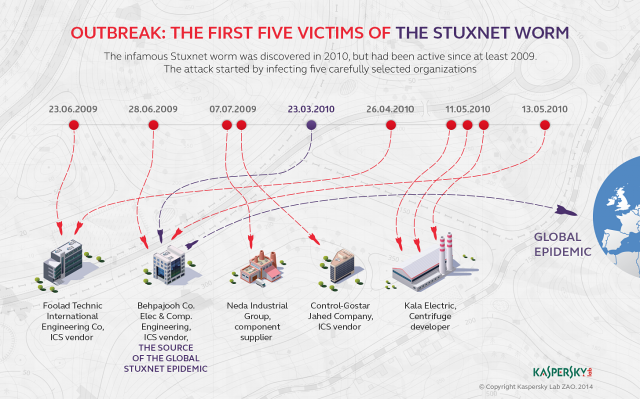
## History

In January 2010, many world governments were nervous about Iran’s nuclear program. But the Iranians were having problems of their own. The centrifuges they used to enrich Uranium were spontaneously breaking apart for no apparent reason. Without the centrifuges, Iran could not create nuclear weapons. Scientists and engineers were fired as officials accused them of manufacturing errors or sabotage (National Public Radio, 2016).

At the same time the Iranian centrifuges were being destroyed, a Belarusian security firm called VirusBlokAda reported a dangerous new type of malware they called “Stuxnet”. One month later, Microsoft confirmed the existence and danger of the Stuxnet, and warned people that the virus was actively targeting the industrial control systems of manufacturing and utility firms (Keizer, G., 2010). Stuxnet was destroying the centrifuges through clever programming and the use of several zero-day exploits.

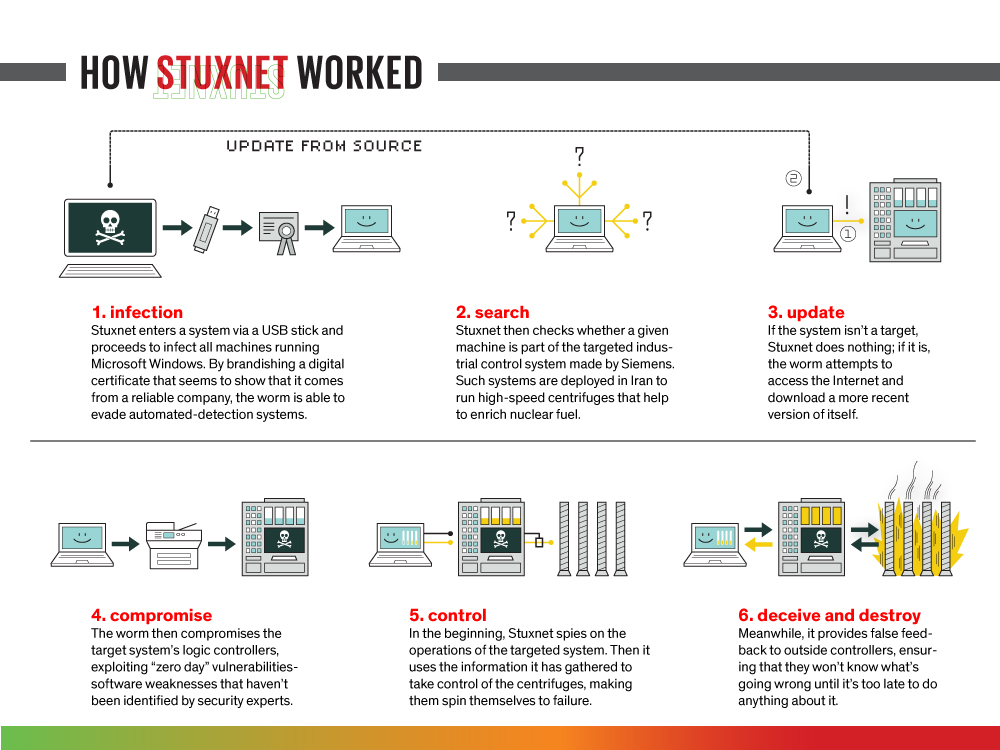
The discovery is interesting because it coincides with a distributed denial of service attack on two of the industrial-control-systems security mailing lists. In fact, the DDOS attack happened directly after the disclosure of Stuxnet. Though the perpetrator of the DDOS attack has never been identified, it may be surmised that the DDOS attack was done to reduce the ability of the Stuxnet victims to react to Stuxnet.

Later that year Microsoft patched two of these exploits and released a statement that they would fix the other exploits later. But a new front warfare had already been discovered. Stuxnet was the first piece of malware known to cause physical harm in the real world, but it would not be the last.



## Purpose and Method of Operation

Researchers believe Stuxnet started off as a program in a USB stick. Various thumb drives containing Stuxnet were dropped outside of vendors servicing the Iranian nuclear program. Once on a vendor’s internal network, the virus could then multiply and hopefully spread into the control systems of the Iranian centrifuges. This allowed Stuxnet to bypass the air gaps protecting the Iranian networks.



Once inside a computer, Stuxnet begins to multiply using several different methods. It copied itself onto open file shares. It copied itself to devices connected to networks the computer was on, using the Windows RPC service. Stuxnet had two different methods to propagate using Siemens database software, embedding itself into datafiles. Finally, it had a peer to peer updating function, allowing it to get stronger over time.

Stuxnet would attempt to multiply until it touched an appropriate target. It would check if the hardware was controlling at least 155 total frequency converters which was an identifying feature of the Iranian nuclear refinement. Next, it would check if the centrifuges were running between 800 to 1200 hertz for thirteen days. In order to enrich nuclear fuel, centrifuges need to run at this rate, and in fact, centrifuges that can run at this rate are export limited by the US government.

Once Stuxnet has confirmed that it is on a target computer, it starts it destructive operations. Stuxnet forced the centrifuges to rotate at irregular speeds that induced excessive vibrations in the centrifuges, which destroyed the centrifuges. It did so slowly, waiting 27 days between vibrations to ensure technicians did not notice anything wrong while simultaneously feeding the monitoring systems fake data.

In 2009, it was estimated the Iranian nuclear program had 7,052 centrifuges, with 4,920 enriching gas. By August, it was estimated only 3,936 were enriching gas, a drop of almost 1000 machines. It was clear Stuxnet had done its job (NJCCIC, 2017).

## Notable Aspects of Stuxnet

Stuxnet is notable for several reasons. This program was the first example of malware being used to cause physical damage. Though malware had existed before, it had been limited to more traditional roles - either software damage or information espionage. However, Stuxnet was actually able to destroy equipment.

Next, Stuxnet was a directed attack. It was actively checking if the host was of a specific type, and it refused to attack if the target was not of the specified types. This indicated a level of professionalism and insider information on the targets that required a certain level of intelligence.

Finally, Stuxnet employed a new method of attack by compromising digital safety systems. The method was generic, and had nothing to do with the Iranian nuclear program specifically. Theoretically, a generic worm could also fake the outputs of digital safety systems and also cause catastrophic failures in power plants and other public utilities around the world.

Because of these reasons, many researchers believe Stuxnet is the result of collaboration between Israel and the US government. The depth, complexity, and resources required imply an organization with vast amounts of resources. For example, the virus faked security certificates from manufacturers. These security certificates should be stored in secured data vaults and never allowed outside the organization.

Conclusion

While cyberwar and cyberterror refer to distinctly different matters, both are rising quickly to prominence in the field of information security. Just as private-sector organizations can be hacked by bad actors, public-sector organizations, including national governments, can experience attacks as well through cyberwar. The cyberspace is emerging as a new battlefield; it is important that as information security professionals, we work towards protecting against these forces to ensure that the cyberspace can remain a useful tool for all.

# 

# References

Banerjea, Aparna. (2018, August 27). *NotPetya: How a Russian Malware Created the World's Worst Cyberattack Ever*. Retrieved from: <https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html>

Garamone, J. (2019, September 20). Esper Describes DOD's Increased Cyber Offensive Strategy. Retrieved from https://www.defense.gov/explore/story/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/

Goodin, D. (2014, November 11). *Stuxnet worm infected high-profile targets before hitting Iran nukes.* Retrieved from Ars Technica: <https://arstechnica.com/information-technology/2014/11/stuxnet-worm-infected-high-profile-targets-before-hitting-iran-nukes/>

Greenberg, Andy. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Retrieved from: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

For High Value targets Chapter 7 https://link.springer.com/content/pdf/10.1007%2F978-1-4939-0962-9.pdf

Gross, M. J. (2011, March). A Declaration of Cyber-War. Retrieved from Vanity Fair: <https://www.vanityfair.com/news/2011/03/stuxnet-201104>

Keizer, G. (2010, September 16). Is Stuxnet the 'best' malware ever? Retrieved from Infoworld: [https://www.infoworld.com/article/2626009/is-stuxnet-the--best--malware-ever-.html](https://www.infoworld.com/article/2626009/is-stuxnet-the--best--malware-ever-.html%5C)

Mahood, S. & Rane, H. (2017) Islamist narratives in ISIS recruitment propaganda, The Journal of International Communication, 23:1, 15-35, DOI: [10.1080/13216597.2016.1263231](https://doi.org/10.1080/13216597.2016.1263231)

Marsili, M. (2019) The War on Cyberterrorism, Democracy and Security, 15:2, 172-199, DOI: [10.1080/17419166.2018.1496826](https://doi.org/10.1080/17419166.2018.1496826)

Microsoft. (2017, October 3). *Advanced Threat Analytics Security Research Network Technical Analysis: NotPetya.* Retrieved from: <https://www.microsoft.com/security/blog/2017/10/03/advanced-threat-analytics-security-research-network-technical-analysis-notpetya/>

National Public Radio. (2016, July 4). Documentary Explores The Cyber-War Secrets Of Stuxnet. Retrieved from NPR: National Public Radio: https://www.npr.org/2016/07/04/484713086/documentary-explores-the-cyber-war-secrets-of-stuxnet

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL. (2017, August 10). *Stuxnet.* Retrieved from NJCCIC: <https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet>

Perlroth, Nicole and Sanger, David. (2019, June 15). *U.S. Escalates Online Attacks on Russia’s Power Grid.* Retrieved from: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>

Scanlon, J. R., & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. Security Informatics, 3(1), 1-10. doi:http://dx.doi.org/10.1186/s13388-014- 0005-5

Standford. (2012, May 8). Dissecting Stuxnet. Retrieved from Youtube: <https://www.youtube.com/watch?v=DDH4m6M-ZIU>