University of Guyana

CSE2203 (2017 – 2018)

Estonia Network Debacle

Massive Estonian Web Failure in 2007

Farnaz Baksh [redacted]

Kim Shing Chong [redacted]

Shemar Brandon Austin [redacted]

Shomari Williams [redacted]

Dwight Ferguson [redacted]

Group E

4/29/2018

Table of Content

1. Introduction

Estonia was known to be the most technologically advanced nation in the World. 98% of the country's territory relied on the internet by different means. Estonia's economy relied on the Information and Communication Technology (ICT) sectors such as e-banking, e-media, e-governance and lastly introduced was their e-voting services. Estonia became the first country to implement online voting for parliamentary elections. Estonia banking process is mostly done over the internet. According to some numbers, 99% of banking transactions were conducted through online banking. Introducing these services online made Estonia vulnerable to cyber-attacks. The country had experienced a major cyber-attack in April-May, 2007 which severely damaged most of the ICT Infrastructure developed. According to the reports, these attacks were said to be politically motivated and conducted by the Russian Government over some political issues.

2. Background

Estonia is located in Northern Europe and is surrounded by Russia, Latvia and Finland. The Capital City is Tallinn. Estonia gained their independence in 1918. Before gaining their Independence, the country was once ruled in the Middle Ages by Denmark, The German Knights of the Livonian Order, Sweden and forcefully ended up as a part of the Russian Empire in the 18th century. In 1920 Russian and Estonia signed a Peace Treaty which ended the Estonian War of Independence. Estonia was forced into the Soviet Union in 1940, which allowed the Russian Government to station 25,000 troops in Estonia to aid in Defense and Mutual Assistance. In 1947, the Soviet Union built a Bronze Statue Soldier originally called 'Monument to the Liberators' in Tallinn, in Estonia to commemorate the Soldiers that died in World War II. Russia became the Russian Federation following the dissolution of the Soviet Union in 1991. It was at that time, Estonia regained their freedom.

In 2007, Estonia and Russia were experiencing conflicts based upon a Treaty in 1949 when Estonia had accepted the Military Graves Protection Act coming from Geneva Conventions. The law stated was about the protection of victims and graves of armed conflicts. After the confliction with the Russian Federation on April 27th, Estonia decided to relocate the Bronze Soldier Monument as it was seen as an oppressive occupation for the Estonians. The Russians dwelling in Estonia saw the movement as disrespectful to their culture and decided to strike by starting riots. According to Spiegel Online (2007, April) – "Around 1500 people gathered in downtown Tallinn to protest against authorities' plans to move the controversial war memorial Bronze Solider to a new location". The riots were dealt with in a quick manner, hundreds were arrested, and reports states that one person was killed. It seemed as though the Russians were not satisfied with rioting only to warn the Estonian Government about their interference with the Bronze Monument.

On April 27th, a number of Estonian Government Officials could not access their emails and websites that were work related. Even to the Estonians were having trouble accessing their ICT services online. The Estonians thought that the problem could have been fixed within hours, but days lived on and the attacks continued and it became apparent that Estonia was under a serious cyber-attack. The attacks lasted for 3 weeks, finishing on May 18th, 2007. Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of cyber-attack. The attack was called Distributed Denial of Service where by massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers causing the servers to become unresponsive. This type of attack involves the use of many computers performing several actions at the same time. The Estonian Government was quick to blame the Russians for such activities conducted.

In order for Estonia to overcome the cyber-attacks, government officials and cyber defense officials who were involved in Cyber Security were brought together to find solutions in protecting the services online from any other form of cyber-attacks. With the help of North Atlantic Treaty Organization (NATO), policies and laws were set. Estonia had requested to the European Union for cyber-attacks to become a criminal offense. The bill was to assist other countries in the future that are susceptible to cyber-attacks. In 2008, Estonia established a Cyber Defense Research Centre in Tallinn to educate and train individuals becoming expertise within the Cyber Security Field.

Estonia was known as the first country to experience a cyber-attack/cyber warfare. The attack helped the Estonians to widen their knowledge, and to strengthen their online services in case of any future cyber-attacks. The attack also helped Estonians to become experts in Cyber Defense today. The most wired country in the world today have become stronger in protecting their services online.

3. Cyber Crime, Information Warfare, Cyber Warfare

There is no single definition for *cybercrime* but the one most commonly known is that cyber-crime are criminal activities carried out by means of computers or the internet and it may target an individual or groups of individuals. Cyber-criminals exploit the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities that cause serious harm and pose very real threat to anyone from any part of the world.

Information warfare can be defined as the use of information strategically to gain an advantage over a particular target. It involves stealing information or modifying information to hurt and destroy the target's reputation. The act of interfering with information is deliberate since it seeks to hurt. Information warfare is first offensive move before a physical attack can be conducted. Information in an organization or to a person is critical, and it is important to protect information by all means to safeguard reputation and critical data that will cause harm in any way.

Cyber-warfare is similar to cybercrime but is most times politically motivated and most times tend to happen on a larger scale attacking military and media stations, parliament or sometimes even critical safety systems such as traffic lights and power grids. As you can see, cyber-warfare doesn't just affect individuals like cyber-crime, it affects governments, companies and sometimes even entire countries and can cause millions of dollars in damage. The rapid computerization of the world has changed the landscape of security and we now rely on computers for almost everything we do in everyday life for some people it is the only way to stay alive.

Estonia is a county that is dependent on computers and in 2007 they experienced one of the worst cyber-attacks in history. For a few weeks the Estonian Internet Infrastructure was subjected to massive DDOS attacks which targeted banks, parliaments and other government sites that were important to the country. These attacks are believed to have been a retaliation by the Russians due to political conflicts. The Estonian government moved a controversial Soviet-era war memorial statue from a square in the city Tallinn to a more secluded location. This caused an uproar with the Russian government and might have been the reason for the cyber-attacks.

Finally, the ultimate question: Was the Estonia attack a cyber-crime, information-warfare or cyber-warfare? Due to the nature and reasons behind the attacks (When and why it was said to happen) it was concluded that the cyber-attack on Estonia was an act of cyber-warfare said to be launched by the Russians.

4. The Method of Attack and Implementation

The attacks, mainly took the form of several targeted distributed denial of services attacks (DDoS), targeted at mainly government ministries and organizations, but still affected Estonian citizens to some extent. These attacks began around 10pm on April 27th, 2007. Initial signs of cyber-attack on the country, involved persons having their email being "spammed" with either junk mail or phishing mails. Soon after government websites were defaced and hacked. Servers became so slow that access to any government site was practically impossible.

The attacks came in two main phases. The first wave was carried out by several "anonymous" persons who would've ran several scripts that were made public, in light of recent riots that were occurring in relation to the moving of the war monument. Parliament email servers were overloaded with requests, government websites were either shutdown or defaced, and news outlets and majority of Estonia's media outlets were forced to close foreign access to their servers, further limiting Estonia from asking for outside help.

The second phase, known as the main attack, began on April 30th and lasted until May 18th. This attack took the form of four (4) waves, each more intense than the initial first phase of attacks. Attackers started implementing botnets to run the DDoS scripts. With the attackers now being able to produce more intense attacks, they included the Hansabank, now known as Swedbank, which was Estonia's largest bank at the time. The attacks eventually caused the bank server to go offline for round ninety (90) minutes. This small downtime resulted in an estimated is losses of about one million USD.

Unlike a usual DDoS which can span for unending periods of servers being bombarded by requests and malicious traffic, these attacks happened in intervals each last varying amounts of hours, and then followed by a downtime where nothing happened. The implemented attacks, when analyzed

from a technical point of view, were described as being “weak”. This weak is subjective, although these attacks practically stopped Estonia from functioning as a society, in a sense that compared to other DDoS attacks. The attackers used small packets in large quantities, but since the packets were small the requests could’ve been handled and most of the damage was done by the large number of packets delivered as opposed to requests being too much for a server to handle. To put this into perspective, the attacks conducted usually consisted of data packets containing data in Megabyte units, while surveys conducted showed ISPs having to handle DDoS attacks on their systems consistent of packets starting from one gigabyte and up.

5. Estonia Cyberattack Prevention

Numerous entities came together to help counter the cyber warfare attacks against Estonia in 2007. These include government officials such as Estonia's Ministry of Defence to security defence officials such as NATO (North Atlantic Treaty Organization) who join forces to combat the cyberattacks against the *e-country*.

Estonia was among the seven countries that join the North Atlantic Treaty Organization in 2004. NATO contribute to the security of the North Atlantic area and has help in ensuring Estonia's security to be better than ever before. Estonia prompted NATO to enhance its cyber-war capabilities and to establish a Cyber Defense Research Center in Tallinn. The center was established in 2008 and it is now titled North Atlantic Treaty Organization, Cooperative Cyber Defence Center of Excellence (NATO CCD COE). It is home to a diverse group of experts from 20 nations and is the hub of cyber defence expertise providing unique international 360-degree look at cyber defence. NATO and the EU help ensure the stability of Estonia's international position and after the ruckus in 2007, Estonia called on the European Union to make cyberattacks a criminal offense.

Another agency that help protect Estonia's national defense is Estonia's Ministry of Defence. The mission of ministry is to defer attacks against the country and ensure that Estonia is capable of defending itself against external threats. Under is organization lies the EFIS (Estonia Foreign Intelligence Service). The main aim of EFIS is to collect, analyse and report information on Estonia's external security threat. They also help in security policy making.

6. Security Defence for Guyana

Overall, the presence of cyberwar is undeniable and every country has to take action to address threat in the cyber realm. Guyana should not be an exception, after all more citizens are getting online daily. Slowly but surely the government officials are taking a step in the right direction.

In March of 2017, the Guyana Police Force try to establish a Cyber-Security Center with the aim to deal with cyber threats and tackle cybercrimes. In December of the same year, Guyana hosted the 16th Caribbean Nations Security Conference (CANSEC) – a forum for high ranking military officials from across the region to get together and discuss critical security issues.

And finally, the Cyber Crime Bill which was first laid in 2016, was return to the floor of Guyana's National Assembly just a few days ago.

Nevertheless, more needs to be done in the cyber defence field if Guyana is to ever put defence measures into place for future cyberattacks. Establishing a Ministry of Defence or being more involved in our association with regional security bodies should also be discussed by our officials.

7. International Cyberattack Prevention

The development of network technology has made it possible for individuals and organizations to be able to share data with each other regardless of their position on Earth. The development of such a privilege has subsequently created a new type of criminal one's whose acts of crime are not bounded to any one territory. The term "hacker" is a generic term to describe people who are adept at manipulating and attacking computers and networks (Denning, 2006). With the existence of these hackers and boundless data communication from territory to territory there must be some lawful control mechanisms in place to protect persons from being the victim of a cyber-attack. For international control mechanisms to be possible the creator of such a mechanism should seek a solution from an objective point of view putting aside territory's beliefs, norms and values. The omission of beliefs, norms and values guarantees a solution that is unbiased and most likely to be the most effective and as such the writer proposes three possible solutions that will be extrapolated on. The three proposed solutions are internationally accepted and endorsed legislation, restrictions on governmental web resources and cyber security assistance

For one to be able to understand why the proposed internationally accepted and endorsed legislation will work one must first understand the prosecution mechanism in place that handles individuals belonging to one country committing a crime against a person outside of the attacker's country. If one is to commit a cyber-crime from his/her country against a target in another country, the attacker is only prosecutable against the laws of the country that they are currently a citizen of. This does not stand true for all countries because of the existence of bodies constructed by the leaders of involved countries that prohibit the assailant from being prosecuted by inconsistent legalization. Instead the countries have shared cyber security laws that eradicated the possibility of a safe haven, one such body is the G8. The use of the words "involved bodies" calls for concern

this is because all countries are not involved in such cross territory agreements leaving the possibility that a person is able to commit a crime and avoid prosecution because of the non-existence of legislation for their act, one such country is Guyana. The internationally accepted and endorsed legislation will ensure that no safe heaven exists for anyone with the capability to commit a cyber-crime it also ensures that the punishment for these crimes remain consistent regardless of where the attacker is in the world as to avoid inconsistent punishments that will have a lesser levied effect on the attacker.

Governmental web resources are extremely important collections of information and at times the backbone of the ministry/governmental body that is affiliated with. At current most governmental web resources from a plethora of countries are available for viewing by persons who are outside of the country, to the naked eye this may seem harmless but one of cyber security technical knowledge would accurately be able to say that this ability is far from harmless. The existence of attacks such as the distributed denial of service (DDoS) attack of which allows an attacker to flood the target's web resource with traffic subsequently slowing it down or in extreme cases causing the complete halt to the web resource making it inaccessible is a cause of concern and should be handled with the highest priority. Tracking the attacker of a DDoS attack relies mostly on the acquiring of the IP addresses involved in the attack to be able to figure out the IP address that is the origin of the attack. The proposed solution to only allow persons within the country to be able to access governmental web resources does not fully eradicate the possibility of a DDoS attack being carried out, however, it does allow for investigators to have a narrower search if these attacks are carried out heightening the possibility of the attacker being caught and prosecuted.

Many third world countries where the probability of a cyber security attack being carried out has little to no cyber security laws thus unintentionally creating a non-prosecutable zone where

attackers are able to carry out attacks exists. The creation of laws encompasses the probability of some act considered dangerous to citizens or to the country as a whole, if the probability is high then the law is created if the probability is nonexistent then there is no need for the law. Countries such as Guyana have only now began to teach cyber security creating professionals who are able to investigate cyber-attack and those who are able to carry out the attack, only now making the need for cyber security laws be considered. The writer proposes that super power countries with already established legislation and punishment attached to the laws to adopt the country's prosecutable criminals and prosecute them accordingly. The adopter country will investigate and trail the hacker and according to their laws recommend the punishment that is attached to the crime to the adopted country. This solution will be affective because the super powered countries already have experience with dealing with criminals of this nature and will be able to accurately deal with such a crime.

8. Reference

About Cyber Defence Centre. (2017, February 02).

Retrieved from https://ccdcoe.org/about-us.html

Cyber warfare is growing. We need rules to protect ourselves. (2018, February 20).

Retrieved from https://futurism.com/cyber-warfare-rules-protect-ourselves/

Cybercrime. (n.d.).

Retrieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

DaSilva, M. (2017, March 29). Police to establish cybercrime unit here.

Retrieved from http://guyanachronicle.com/2017/03/27/police-to-establish-cybercrime-unit-here

Denning, D. E. (2006). *Information warfare and security*. Boston: Addison-Wesley.

E-Banking. (n.d.).

Retrieved from https://e-estonia.com/solutions/business-and-finance/e-banking/

Estonia and NATO. (n.d.).

Retrieved from http://vm.ee/en/estonia-and-nato

Estonia country profile. (2017, November 30).

Retrieved from http://www.bbc.com/news/world-europe-17220810

McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia.

Retrieved from http://www.bbc.com/news/39655415

Schmidt, A. (2013). *The Estonian Cyberattacks*. [PDF FILE]

SPIEGEL ONLINE. (2007, April 27). Deadly Riots in Tallinn: Soviet Memorial Causes Rift between Estonia and Russia - SPIEGEL ONLINE - International.

Retrieved from http://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html

U.S Libray of Congress (n.d.). *The Soviet Era 1940-85.*

Retrieved from http://countrystudies.us/estonia/3.htm

What is Cyberwarfare (Cyber War)? - Definition from Techopedia. (n.d.).

Retrieved from https://www.techopedia.com/definition/13600/cyberwarfare