MUNESCO

Forum: GC5- Communication and Information
Issue: The issue of abuse of cyber power with a special emphasis on the US and Russia.
Student Officer: Kiyan Rezazadeh
Position: Deputy Chair

Introduction

Since the rise of networking, there have been many legislations and regulations passed on cyber security and data protection. Not only limited to national legislation, but international. These regulations and legislations have been placed due to individuals, corporations and governments have used their cyber power to harm others or for gain of more power, whether it is political or financial. Today, many security breaches have been placed in Intranets, Extranets and the Internet. Even though networks and alike are safer than ever, the issue at hand is still ongoing and for countless years, many governments have faced accusations of using their cyber power to rig elections and for the gain of their country. The most well-known example of such accusations being the 2016 presidential elections held in the United States of America having Russian Interference. However, from 1946 to 2000, the USA had intervened with 81 foreign elections [1].

However, the only issue is not only government-related, 67% of all business-related crimes committed were related to cybercrime [2] in 2005. Similarly, in 2019, the revenue lost by cybercrime globally was estimated to be 5.2 trillion US Dollars [3]. The most recent governmental related cybercrime took place in December 2019 where New York Times have found an application of the UAE was setup to be a spying tool [4].

Definition of Key Terms

Cyberwarfare: The use of cyber power and technology to attack a nation/state. Cyberwarfare is usually carried out to cause physical complications.

Cyberterrorism: "Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage." (Catherine A. Theohary & John W. Rollins 2015)

Cyberattacks: An attack carried out on networks to damage, steal or replicate copies of the information they contain. Cyberattacks are also used to immobilize networks to harm the organization who owns the network whether it is to reduce the income, followed by stealing the income, or it can be carried out to harm the individuals who use the network by stealing their information.

Cyberspies: Individuals or organizations who steal or observe data without the permission of the data holder or what the data is based on, cyberspying is most commonly done via spyware softwares. Targets of cyberspying are usually individuals, rivals, companies, government officials and military personnel, cyberespionage.

Spyware: Unwanted devices or softwares that interact with computers, databases, and servers which are used to view and collect data. Spyware are the tools that are used for cyberespionage.

Cyber Extortion: The act of committing an internet crime to demand needs from an individual or organization by threatening to or causing harm to them.[5]

Malware: Short for malicious software, malware is an umbrella term for any software which intentionally causes harm or threatens the safety, identity and data of an individual, organization or government. Examples of malware include: viruses, spyware, ransomware, and trojan viruses.

Phishing/Pharming: Phishing is a fraudulent act of obtaining information on an entity by sending spam emails, fake text messages, or scamming/ Pharming is phishing done on a larger scale and may also involve hacking websites.

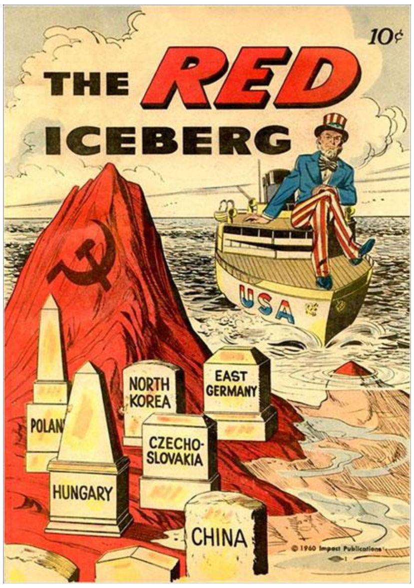
Ransomware: Ransomware is a malware which takes over a computer or database, either corrupts, locks, threatens to publish their information or completely deletes data and which the victim has the pay a sum to the owner of the ransomware.

Background Information

After World War 2, there has been rivalry between the USA and Russia (ex. USSR). Whether it was the space race, the Vietnam war, the Cold war or recently until 2016 where USA and Russia had tensions and had major part in the cause of the Syrian civil war. However, these problems are mostly physical, there are countless examples of tensions between these countries which have occurred over the internet and with the usage of cyber power.

Summary of tensions:

The first conflict that had occurred between the US and USSR was post-war in 1947 when the two powers had entered the Cold war. Throughout the Cold war, the two powers would spend billions in research and development to spy on each other. This trend of espionage would continue well after the USSR has broken up and the Cold war would be over.



Whilst the Cold war was being carried out, there was a war starting between North and South Vietnam. Similar to USA and USSR, one side was communist whilst the other side was anti-communist. Naturally, the US and USSR allied with the side their government had the same ideology with and this further drove up the rivalry.

Originating from the nuclear arms race, the space race of the 1960s and the 1970s was a prime example of these two superpowers competing. The space race had officially begun on August 2, 1955, when USA has announced their interest in launching satellites into earth's orbit, merely four days before the USSR released a statement. USSR was in the lead of the competition as they had launched their satellite, Sputnik 1, before USA launched their satellites and USSR had sent the first man in space, Yuri Gagarin. However, it is said that the USA has won the space race.

With the collapse of the USSR, the rise of the information age brought by the internet and the end of the Cold War. The tensions continued into our modern world.

Current tensions:

With the rise of the internet, the affairs between the two nations have been carried to technology. Espionage which had been carried out during the Cold war had become Cyberespionage, the invention of spyware occurred, and international intervention of presidential elections have been higher than ever. A famous example of international intervention of governmental elections was in 2016 where a group of hackers which had affiliation with the Russian government were accused of leaking emails sent out by Hilary Clinton, one of the presidential candidates. An investigation was carried out by the United States intelligence agencies had proved the claims that the hackers were related to the Russian Government's military intelligence service (GRU). However, the USA has been accused of interfering with governmental elections in other countries as well. It is claimed that the US has interfered with 81 foreign elections when compared to Russia and USSR's total of 36 interventions, since 1946. Even though the US has more interventions, they are that of smaller governments such as Bolivia, which the US interfered in 2002.

Not only are elections being intervened by other governments, there have been large-scale cyber attacks carried out to governments and large corporations closely related to governments. As recently as October 2019, Russia has been accused of carrying out a cyberattack on the Republic of Georgia which took down multiple Georgian websites and crashed many servers. A follow up has been made by the government of Australia and the United Kingdom by wanting to deter Russia from interfering with the 2020 elections which will happen in the United States [6]. The Russian government has carried out cyberattacks on member states such as: France, Russia, Germany, Poland, Ukraine, Estonia and most recently, Georgia. Currently, there are no cyberattacks which have been linked to the US government. However, it has been conspired that the other presidential candidates knew about the email leaks prior to them occurring however it has never been proven to be correct.

Timeline of Major Events

January 1, 1983	A series of networks were assembled which connected with each other. This was the first form of the Internet.
1989	The modern version of the Internet was created, dubbed "World Wide Web".
1991	The Cold war came to an end with the collapse of USSR and espionage started to transform, into cyberespionage due to the information age starting.
July 16, 1998	Data Protection Act of 1998 was passed in the UK, preventing corporations to distribute data of their users.
October 17, 2000	The Information Technology Act of 2000 was passed in India, covering legal issues regarding networks and protecting constitutional rights.
November 23, 2001	Budapest Convention was signed, being one the first international treaties on cybercrimes, which then was enacted in 2004.
March 1, 2006	Additional Protocol to the Convention on Cybercrime was added to the Budapest Convention which tackled xenophobia and racism online.

May 2, 2007	Estonia experienced a cyberattack by Russia, taking down large websites.
April 2015	Paris-based TV network TV5Monde was hacked in attempt to take down the 12 channels they aired.
June 29, 2015	A 55,000-page email was discovered which contained classified information which was later linked with Hillary Clinton
March 19, 2016- April 2016	Hillary Clinton's campaign chairman John Podesta received a phishing email which eventually caused hackers to gain access to his Google account which ultimately is used to create a fake mail to further phish Hillary Clinton's staffers which the hackers gained their credentials which was when the documents and emails were leaked.
July 25, 2016	FBI launches an investigation to find the hackers
December 9, 2016	CIA determines that the Russian Government was affiliated with the email leaks to boost Trumps reputation and harm Clinton. However, Trump's team dismissed CIA's claim

Major Countries and Organizations Involved

Russia:

Russia has been one of the major countries which has association with hacking groups and furthermore one of the countries which has been a part of many cyberattacks and security breaches.

USA:

The USA has been victim to cyberattacks, the most infamous being the elections. As a superpower, the USA has many corporations, governmental and privately owned, which tackle the issue of cyberattacks and hacking such as the pioneers of antivirus softwares being mostly founded in the USA. However, the USA has government branches such as the NSA, which has been proven to spy on their citizens.

UN:

The UN has discussed the issue of cybersecurity and has passed resolutions on the matter previously. UN has also setup unions such as the Information Technology Union (ITU) which has affiliation with ECOSOC.

European Cyber Security Organisation (ECSO):

ECSO is an NGO which has been formed under Belgian Law which is fully self-financed, which has been contracted by the European Commission for the Cyber Security contractual Public-Private Partnership (cPPP). ECSO has shareholders such as large companies and universities. EXO's main focus is to create a safe cyber environment and to support the European Digital Single Market by finding trustworthy cybersecurity solutions [7].

International Security System Association (ISSA):

The ISSA is an international NGO which focuses on protecting information, promoting a secure digital world and promoting cybersecurity on a global basis. ISSA also wants to achieve to protect full digital societies and they also educate individuals and corporations on cybersecurity.

SANS Institute:

SANS Institute is a profited-organization which is privately owned which was founded in 1989 which focuses on protecting data, giving cybersecurity training and sell certificates (Certificates are the best way to tell whether the website you enter is safe. Websites with certificates will have lock icons in their URL and begin with https://, all major websites have certificates.) SANS Institute offers courses on topics such as network defence and cybersecurity.

Previous Attempts to Solve the Issue

Resolution of the General Assembly; Combating the criminal misuse of information technologies
January 22, 2001 (A/RES/55/63)

Combating the criminal misuse of information technologies
January 23, 2002 (A/RES/56/121)

Creation of a global culture of cybersecurity
January 31, 2003 (A/RES/57/239)

Creation of a global culture of cybersecurity and the protection of critical information infrastructures
January 30, 2004 (A/RES/58/199)

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures
March 17, 2010 (A/RES/64/211)

Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat
October 25, 2013 (A/68/552)

Palermo Convention
December 12, 2000

Budapest Convention
November 23, 2001

Additional Protocol to the Convention on Cybercrime
March 1, 2006

Possible Solutions

- Propose new resolutions based on cybersecurity rather than cyberpower since those two are closely related

- Providing new seminar/conventions to raise public awareness, similar to ISSA or SANS Institute
- Finding a common ground between the two superpowers in mind when making new clauses
- Similar to ITU, there could be a new branch or sub-branch of UN which directly tackles cybersecurity and cyberpower.
- Related to the 2016 elections, having UN forces or a similar non-biased party count the presidential or important votes to prevent events similar to 2016
- Introducing software for government officials so that their sensitive information stays safe rather than having to rely on civilian products and corporations.

Useful Links for Further Research

1. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

2. https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

3. https://www.issa.org/about-issa/

4. https://www.cisecurity.org/cybersecurity-best-practices/

5. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

6. https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

7. https://www.bbc.com/news/world-us-canada-44825345\

8. https://fas.org/sgp/crs/natsec/R43955.pdf

9. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

10. https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia

Bibliography

[1] Foreign Electoral Intervention
https://en.wikipedia.org/wiki/Foreign_electoral_intervention

[2] Cybercrime
https://www.bjs.gov/index.cfm?ty=tp&tid=41

[3] This Is the Crippling Cost of Cybercrime on Corporations
Iman Ghosh - https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/

[4] Chat App Totok Is Spy Tool For Uae – Report: Silicon Uk Tech News
Tom Jowitt - https://www.silicon.co.uk/mobility/mobile-apps/totok-spy-tool-for-uae-325873

[5] Cyberextortion Law and Legal Definition -
US Legal, Inc - https://definitions.uslegal.com/c/cyberextortion/

[6] U.S. and Allies Blame Russia For Cyberattack on Georgia
David Sanger-Marc Santora - https://www.nytimes.com/2020/02/20/world/europe/georgia-cyberattack-russia.html

[7] About ECSO -
https://ecs-org.eu/about