Committee: Security Council

Issue: Cyber-terrorism

Student Officer: Chris Moustakis

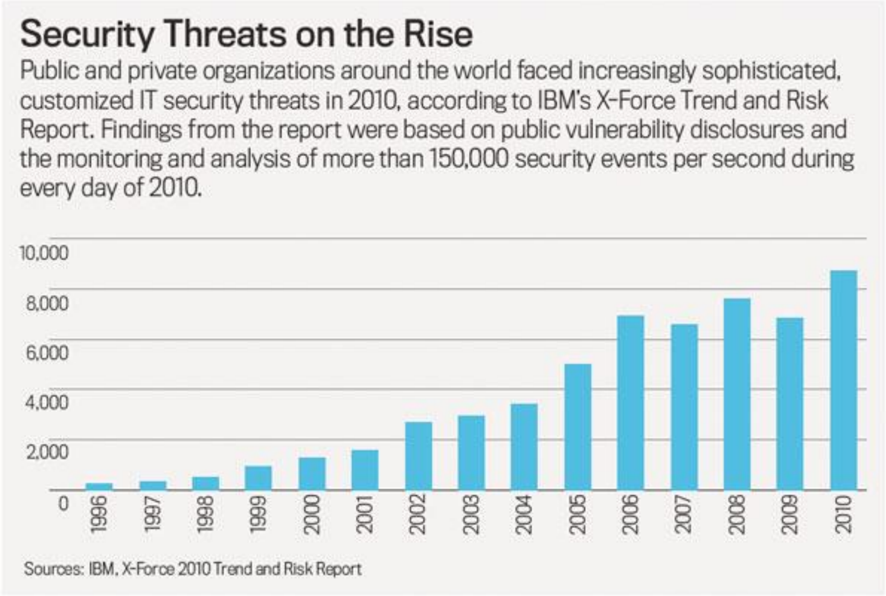
Position: Deputy President

INTRODUCTION

In the last decades, the extraordinary advancements made in technology and the ever increasing rate at which technology is evolving contributes to large shifts in the way we interpret and understand our world. However, the benefits of technology can be turned against us through cyber-attacks, industrial manipulation and even recruitment of individuals for terrorist groups using the amazing ability to connect with others from all around the globe.

All of the above are called acts of cyber-terrorism. It is a very important topic in our day and age, as it has recently arisen and the United Nations have yet to address it in a comprehensive and interdisciplinary manner. It is a very challenging issue that has been recently proven urgent.

As of now, its effects have spread across the globe and have terrorized people, businesses and governments, as they understand the potential damage that can be caused. If this issue is not resolved, the people with the necessary skills could manipulate governments and disrupt peace, something extremely negative for our future, if we wish to progress as a civilization.



Security Threats on the Rise

Public and private organizations around the world faced increasingly sophisticated, customized IT security threats in 2010, according to IBM's X-Force Trend and Risk Report. Findings from the report were based on public vulnerability disclosures and the monitoring and analysis of more than 150,000 security events per second during every day of 2010.

Sources: IBM, X-Force 2010 Trend and Risk Report

More specifically, just like we have terrorist groups, we also have cyber-terrorist groups, which are extremely dangerous and carry out some of the most dangerous attacks. Unfortunately, the web offers the ability of anonymity and by disguising the IP addresses, the locations of the terrorists are extremely hard to be specified. Thus, cyber-criminals are almost untraceable and continue their attacks as they are rarely caught. That is one of the main reasons why it is difficult to resolve. Additionally, cyber-attacks are extremely fast and once they have begun, it is difficult to intervene. Even though terrorism is somewhat planned beforehand, cyber-terrorism is much more calculated and precise. It is carefully planned out before the actual attack and if the cyber-security system does not stop the attack, then it is successful. There are no forces to prevent it from accessing data and information. Last but not least, cyber-attacks may not directly hurt individuals, however, their effects are far more harmful to their lives. The 2 different types of terrorism are of course linked. They both hurt nations and both need to be stopped. And as terrorism slowly shifts to the cyber world, the United Nations are called upon to resolve this issue once and for all.

DEFINITION OF KEY TERMS

Cyber-Attack

It is classified as an attempt by hackers to damage or destroy a computer network or system. Countless incidents are reported every day and they are on the rise, slowly creating global terror on the Internet.

Cyber-Security

It substantially is the entirety of the measures taken to protect a computer or computer system against unauthorized access or attack. For example, when a hacker tries to access data without authorization, without firewalls and system security, he would be free to do so and could cause disruption by using that data. Without it, our systems are helpless in case of an attack.

Cyber-Terrorism

The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.A series of cyber-attacks or one large scale cyber-attack with the target being usually aprivate company or a specific government.

Terrorist recruitment

It is the recruitment of new individuals by terrorist groups, in order for them to grow and gain support, therefore increasing their area of influence. This action can now be carried out through the web and is extremely effective, since understandably, the terrorist groups can contact people from anywhere and reach out to more individuals, since the use of technology is very common.

Cyber-Criminal

The individual who unlawfully uses technology to conduct cybercrime operations and the one who creates or uses malicious software to cause disruption. Only 0.3% of cyber-criminals are world-class skilled individuals, however, altogether every single one of them causes disruption, scaling from shutting down a public web-site, to stealing and selling government secrets.

Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network, such as the Internet. It is the basic cyber-defense measure.

BACKGROUND INFORMATION

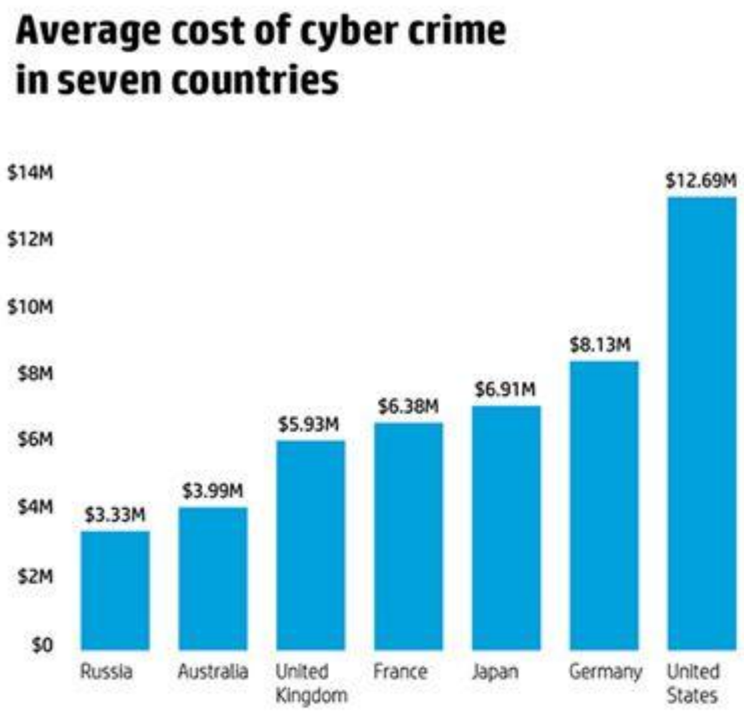
Dependence on technology

As technology progresses and we realize the advantages it offers, we tend to apply it to possibly everything we can, as it helps in the modification of those things towards their improvement and additionally offering ease. This is a contributing factor to why we use it. Cyber-Attacks started almost as soon as modern technology was created and there have been countless attacks on various sectors of the economy and society, like the attack on Canada's agencies or the DDOS attack in Estonia. A way must be found to use technology and its benefits without it being abused as a weakness.

The evolution of cyber-attacks

Already from the 1970s to the 1980s, cybercrime started making its appearance. It started from abusing flaws in systems to exploiting them in order to manipulate individuals or groups of people. But when cyber-crime really began to sky-rocket was with the invention of the web. It revolutionized everything and it created a brand new and more advanced field for abuse and manipulation.

People with the right skills could now have access to data, information and control over important things such as management and organization of a country/company. This was extremely alarming because the full potential of it was not understood. And so, year after year, cybercrime grew with the peak being in 2010 where there were 150,000 incidents every second. The reason that there were so many of them was that sometimes, when a hacker is advanced enough, he/she can construct an automated process through which he/she multitasks and attacks multiple targets at once.



The average costs of cyber crime in seven countries (converted to U.S. dollars for comparison) show that U.S. companies average a significantly higher total cost than in other nations.

Source: The Ponemon Institute, surveying 257 companies

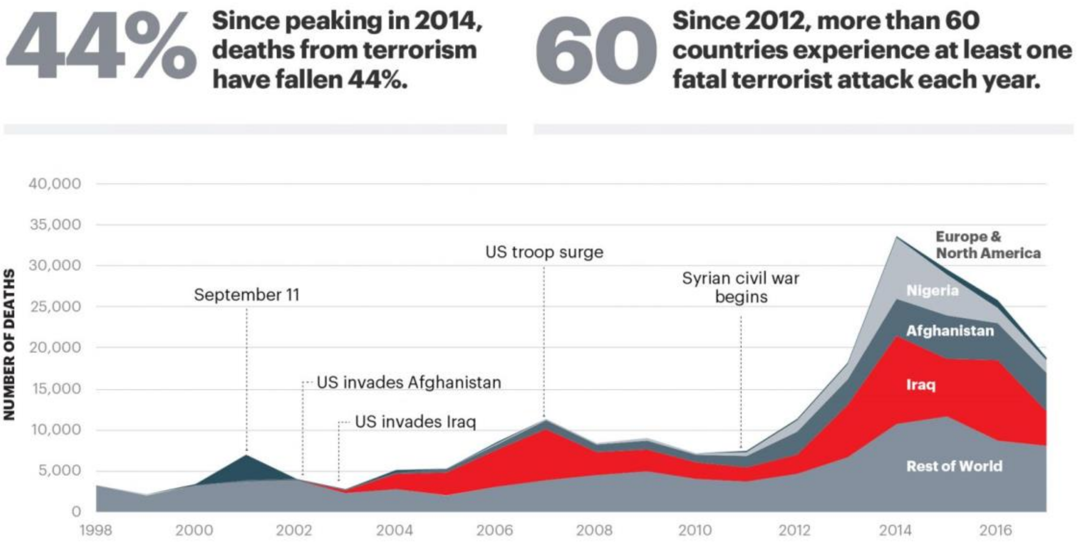
As we can see in the image, cyber-crime creates issues in the economy and is hurtful to nations. The main targets of cyber-crime are usually the P5 members, and so it is easily concluded that they are very involved in this issue at hand. They are also the most aware ones and have taken a lot of means to protect themselves from such attacks as well as create legal framework for cyber-security.

Means to stop cyber-crime

Multiple defense systems and firewalls have already been established to prevent damage from cyber-attacks, however the ever-increasing group of hackers around the world is doing everything they can to bypass them. The first computer firewall was just a simple network composed of very common elements, and yet, it was a huge step towards the creation of cyber-security. Now, although we may have the means to stop cyber-attacks, those means cannot be implemented on a world wide scale. They are far too expensive and need way too many resources for all nations to handle, especially Less Economically Developed Countries (LEDC's). Therefore, we are left with an inadequate solution to a problem for most countries of the world. Seeing that cyber-terrorism is going to be one of the most important problems to ever threaten world peace, it is crucial that one is found.

Terrorist recruitment and the internet

Over the years, a lot of damage has been caused to nations that originated from terrorist groups. The web offers us communication across countries. Although that is a huge step in the world of communication, it also enables terrorist groups to reach out to people. This enables terrorist groups to grow and cause even more damage. Such acts have caused severe damage on countries such as France. Terrorist recruitment is an issue on its own, however, the web makes it easier for it to be carried out. As mentioned in the Definition of key terms, such a tactic is very effective and needs to be stopped or at least minimized.



Source: START GTD, IEP Calculations

Types of cyber-attacks

DDOS attacks: distributed denial-of-service attacks are a very effective in disruption. They refer to making publicly open websites inaccessible. The purpose of such attacks is to essentially silence a website, in case one does not agree with the opinions published. Main targets of this type of attack are government websites, as well as bank and company ones. A good example of a DDOS attack was the one in China, in which a hacker group shut down a very popular search engine.

Cryptojacking: An extreme increase in cryptojacking incidents has been noted since late 2017.This phenomenon can be linked to the high value cryptocurrencies have gained in the past years, therefore allowing hackers to exploit flaws in the systems and profit from cryptocurrencies with activities such as cryptojacking. In case of an infection, victims cannot be aware of the operation of coin miners incorporated into browsers through the use of processing power and thus, the current situation cannot easily be controlled. Essentially, it is when hackers abuse bugs in crypto-currency systems and exploit them to earn money.

There are a lot more types of cyber-attacks, however, most of them are attempts to steal data and information, or some of the ones above. All of them are very harmful, usually at the expense of nations or companies.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America (USA)

Understandably, not only the United States of America have taken a lot of measures against it, they have also been the target of approximately 50% of the attacks. Already, they have invested in cyber-security and have a strong cyber-defense system, which due to the amount of attacks that they are up against, is updated regularly. They have also managed to create legal framework on cyber-security, which most countries have not yet done. They have suffered, as mentioned before, numerous cyber-attacks.

Russian Federation

The Russian Federation is one of the major nations in the world and is also a target of cyber-attacks. Nevertheless, it has created stable cybersecurity, which prevents cyber-attacks from costing too much and keeps them under control. Being a part of many collective efforts to stop cyber-terrorism, it stands as one of the most active nations on the topic.

People's Republic of China

China has been especially involved in this field, as it is a growing economy. That has also enabled it to sustain cyber-security and render itself one of the most protected and cyber secure nations on the planet. Additionally, the nation has developed advanced technology to avoid such attacks. More specifically, they have suffered one of the largest DDOS attacks to ever happen, in 2010, where Iranian hackers hacked a popular search engine in order to pass their political opinions.

France

France has a general connection to terrorism. Other than the amount of cyber-attacks that it is up against, terrorist attacks have been known to strike. Especially when it comes to terrorist recruitment through the web, France is deeply concerned about this issue. Moreover, it has strong cyber-defense, however, it has to withstand several small-scale cyber-attacks every day, making it one of the most threatened countries in the globe.

The United Kingdom

The UK has also been known to make efforts against cyber-terrorism and cyber-crime in general. It is involved and has attempted to resolve the issue multiple times. Additionally and more specifically, it was severed by an attack on its infrastructure and organizations said to be carried out by Iranian hackers.

Office of Counter-Terrorism

This UN organ, as we all know, specifies in combating terrorism. Since cyber-terrorism is one of the main types of terrorism, it is justifiable that this organ is involved and active in this particular field.

TIMELINE OF EVENTS

Date	Description of Event
1988	The Morris Worm, a devastating virus that caused severe damage to the US economy. One of the first ever viruses and the birth of cyber-crime.
1997	The NSA tests the USA's cyber defense system and realizes that it can be easily hacked using commercial computers and tools.
2007	Massive DDOS attack in Estonia, which is deeply hurtful to the government. This attack started to show the potential of cyber-crime and earned its publicity and popularity.
2007	Chinese government reports huge amounts of stolen information by hackers. Once again cybercrime has created national disruption.
2010	Iranian hackers take over a popular search engine in China and display their own political opinions in a message.
2011	Major cyber-attack in Canada mostly targeting its agencies.
2012	Huge Cyber-Attack taking place since 2007 is discovered and is said to have resulted in leaks from all European countries and the Western World.
2013	Cyber-Defense Meeting by NATO officials agree upon the creation of full-proof cyber-protection.
2015	Cyber Attack directed to the White House said to be carried out by Russian hackers. Various information about government employees breached and stolen.
2015-2019	There have not been many large-scale cyber-attacks during this period, there have been, however, at least 3,000 medium-scaled ones every single week.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Convention on Cybercrime by the Council of Europe

Resolution 55/63, January 2001

Combating the criminal misuse of information technologies

Resolution 56/121, January 2002

Combating the criminal misuse of information technologies

Resolution 57/239, January 2003

Creation of a global culture of cybersecurity

Resolution 58/199, January 2004

Creation of a global culture of cybersecurity and the protection of critical information infrastructure

Resolution 64/211, March 2010

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The cyberspace is not limited by any geographical boundaries and thus, it can only be regulated by the international law. The only international treaty to this day is the Convention on Cybercrime by the Council of Europe, which provides for a legal framework for the protection of society against cybercrime. This convention is essential for anti-cyber-terrorism protection to take place and therefore, countries can establish cyber-defense systems and protect their citizens, data and infrastructure. Countries like the USA have done so and have established additional legal framework for protection against cyber-attacks.

POSSIBLE SOLUTIONS

The approach to this issue should be through numerous different points of view. Seeing that this issue is yet to be solved, it is crucial that you address all of them with different clauses.

First of all, we should address the issue of cyber-security and the fact that most of the time it is inadequate. Of course, any clause related to updating computer software provided to government and making cyber-security available to anyone who needs it, starting from businesses should be extremely detailed. Also, in this point of view, delegates should address what happens if a cyber-attack is not stopped by the system's firewall.

Additionally, delegates should consider constructing clauses about how to prevent cyber-attacks from even occurring. That can be implemented by measures such as creating means to identify cyber-terrorists and arrest them or implementing anti-cyber-terrorism campaigns. This part of the issue is extremely important as it is the root of the issue at hand.

Moreover, cybercrime costs nations a lot and deeply hurts the economy. It is advised that the cost of these cyber-attacks is minimized through solutions proposed in clauses. Additionally, it also terrorizes the society and everyone in it.

Last but not least, the recruitment of terrorists through the web should be addressed. That can be done by monitoring social media and websites in order to block any messages related to this topic. Generally, the clauses about this aspect of the issue should be very detailed, taking into consideration its utopic nature. The solution suggested should be feasible and implementable and not abusive of the UN's funds or the other nations.

BIBLIOGRAPHY

"Cybersecurity."*Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/cybersecurity.

"Cyberwar Timeline." *Infoplease*, Infoplease, www.infoplease.com/world/cyberwar-timeline.

"Firewall (Computing)."*Wikipedia*, Wikimedia Foundation, 20 June 2019, en.wikipedia.org/wiki/Firewall_(computing).

"Fundamentals of IT and Cybersecurity Chapter 1 Study Guide."*Quizlet*, quizlet.com/319332669/fundamentals-of-it-and-cybersecurity-chapter-1-study-guide-flash-cards/.

Nato. “The History of Cyber Attacks - a Timeline.”*NATO Review*, www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htmm.

"Privacy And Cybersecurity In Russia - Data Protection - Russian Federation." Articles on Europe - Privacy Including Law, Accountancy, Management Consultancy Issues, 31 Oct. 2018, www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia.

"What is the Internet of Things (IoT)? - Definition from Techopedia."Techopedia.com, www.techopedia.com/definition/28247/internet-ofthings-iot.

"What is a Distributed Denial-of-Service (DDoS) Attack?" Cloudflare, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

"What is Data Protection? - Definition from WhatIs.com."SearchDataBackup, searchdatabackup.techtarget.com/definition/data-protection.

"What Are the Motives Behind Cyber-attackers?" CGS, 26 June 2018, www.cgsinc.com/blog/what-are-motives-behind-cyber-attackers.

IMAGES:
https://www.bing.com/images/search?view=detailV2&id=B0C4426FFC53EC99AEE749B9361CA2AFA533E29F&thid=OIP.Qk3K_SHxrUixDrXei_0oPgHaD9&mediaurl=http%3A%2F%2Fvisionofhumanity.org%2Fapp%2Fuploads%2F2017%2F02%2Fchart3-1600x855.jpg&exph=855&expw=1600&q=terrorist+attacks+graph+2010-2019&selectedindex=0&ajaxhist=0&vt=0&eim=0