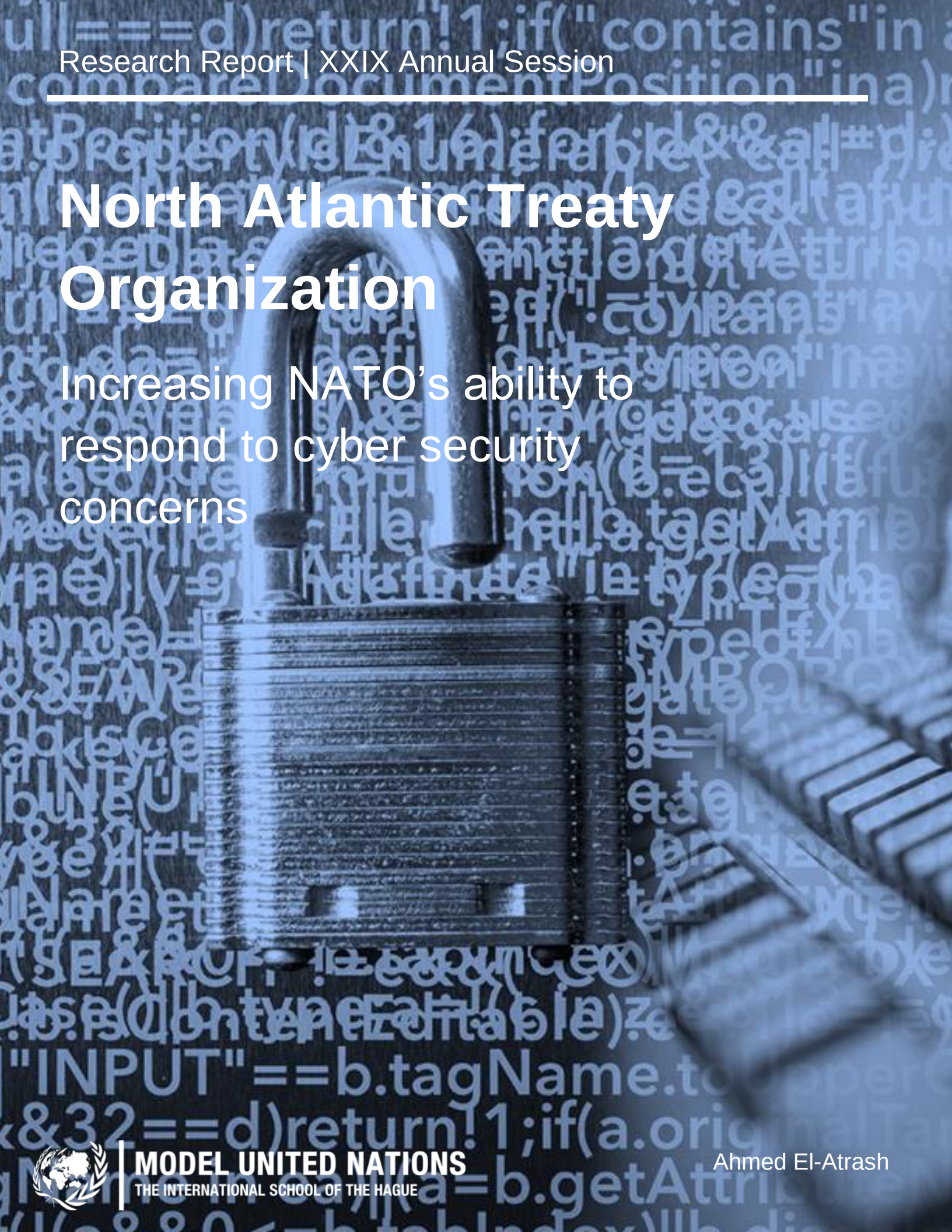
North Atlantic Treaty Organization

Increasing NATO's ability to respond to cyber security concerns



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Ahmed El-Atrash

Forum	NATO
Issue:	Increasing NATO's ability to respond to cyber security concerns
Student Officer:	Ahmed El-Atrash
Position:	President

Introduction

With approximately 4.1 Billion connected to the internet around the world, it has undoubtedly become a feat of human innovation and development. The internet has penetrated and overhauled various sectors of civilization acting as a catalyst for globalization but also the proliferation of social media as a means for global communication. Consequently, the internet has attracted large sums of money to its platforms whether in the form of the $3.5 Trillion projected in online retail for 2019 or the $205 Billion in advertising expenditure which trumps Television by $13 Billion. This has created an environment for financially and politically motivated cybercrime to rise exponentially to the extent that information theft is now the leading crime against organisation. The issue is an ever-evolving one with approximately 150 million malware samples created each year with most being polymorphic in order to avoid detection. In short, there are more threats than ever with one attack every 39 seconds and each new threat being more potent and better at its job than the last. The UN research reported that cyber crime creates almost $1.5M trillion in revenue for criminals annually. The main theme in this research report is highlighting the importance of cooperation between all members in order to fight back against cybercrime. Nations must start sharing cybercrime analytics and data at a higher rate if they want to keep up. This is definitely easier said than done due to the different technological and cybersecurity infrastructures in each respective country. They key is to draft amendments and communiques that aim to make policies as unilateral and inclusive as possible.

Definition of Key Terms

Malware

Short for “Malicious software”, it is a term that describes any form of code that poses a threat to computer systems. There are many types of malware under its umbrella term with notable examples being ransomware which blocks functions until money is paid or Worm Code which spreads from one device to another stealing sensitive information along the way. Further examples can be seen below:

- Spyware (Programmes that steal personal information and log internet usage)
- Adware (Software that bombards you with advertisements and collects data)
- Logic Bombs (Software that destroys files and functions on a device)
- Rootkit (Software made to enter target computer without being detected)
- Zip Bombs (Software that stops and crashes running programmes)

Cybercrime

Any crime committed through computer systems or the internet. It is made up of classical forms of crime such as theft and fraud but has also evolved into newer forms such as Denial of Service attacks and Credit Card cracking. The most complex aspects of cybercrime are the anonymous black market systems for selling cyber-weapons such as botnetworks and viruses but also black markets responsible for sharing Child pornography and on demand hacking services

Hacktivism

Hacking data banks or computer networks in order to progress a certain political goal or intent. While a regular hacker aims to compromise private information and inflict harm. A hacktivist will make use of malware and disruptive software in order to further a political goal by targeting certain websites or networks that they oppose or that they think will bring them attention for their political motive which generally leans towards an anarchist perspective with groups such as Anonymous and Chaos Computer Club being most notable.

IOT (Internet Of Things)

The increasingly growing internet capabilities of devices in a household or public setting. From washing machines to airplane engines, objects and components of objects are becoming smarter and are joining an expansive network of data. It is technologically promising for problems such as waste management and traffic management but the downside is the vulnerability to hacking that it creates. The increased amount of data a person has on their digital footprint makes it a logistical challenge to ensure the security of said information.

Blockchain

In essence, blockchain is a decentralized network of data that specializes in the exchange of data between parties with its primary basis being the bitcoin crypto currency. It works by creating what is called a block when a transaction is requested. This block is then stored and verified on a ledger on millions of other computers at which point it joins a chain of other transactions that occur autonomously. This process removes any middlemen but consequently also removes any regulator parties making it a possible threat in the future as it provides an ideal climate for the movement of black money.

Cyber Terrorism

The use of the internet, public networks or computers in order to cause harm to people or organisations in order to further an ideological or political goal. This usually includes creating alarm or panic through the disruption of large scale networks generally by installing malware such as Worms or Ransomware which spread quickly and cause collateral damage. Cyber terrorism is divided into 3 main groups:

1. Simple Unstructured - Using pre-made tools to attack individual networks
2. Advanced structured - More nuanced attacks on multiple networks with self modified hacking tools
3. Complex Coordinated - Highly coordinated attacks on large scale networks bypassing high level security systems and making use of highly sophisticated hacking tools

Polymorphic Virus

A virus that aims to avoid detection by replicating itself and changing its code structure and content. It mutates to outsmart any existing defenses. This makes dealing with this type of virus a massive and costly challenge because defense code must be continuously rewritten. It is becoming easier to write this kind of virus and thus harder to combat it. In some cases, the code can mutate itself up to 20 times per day to escape detection. The two main ways that security experts combat this code in are:

1. Behaviour Scans - This is where the general behaviour of the polymorphic code and its changes are analyzed instead of looking at the literal code. This means that you can anticipate what the virus will do next.
2. Heuristic Analysis - Analysing a virus and its mutations in order to identify features that they share. This will then be targeted in defense security code.

General Overview

Cyber security threats are continually becoming more widespread, complex and potent. The Alliance is confronted with an evolving threat landscape that is complex in nature. Cyber-attacks have become a prominent component of global developed warfare in the past few years. To fulfill the NATO alliance's core duties of crisis management and insurance of collective safety, NATO and its allies depend on efficient and effective defences against cyber warfare. The alliance must have protocols in place as a collective to protect its systems and members against the increasing potency and complexity of global cyber threat.

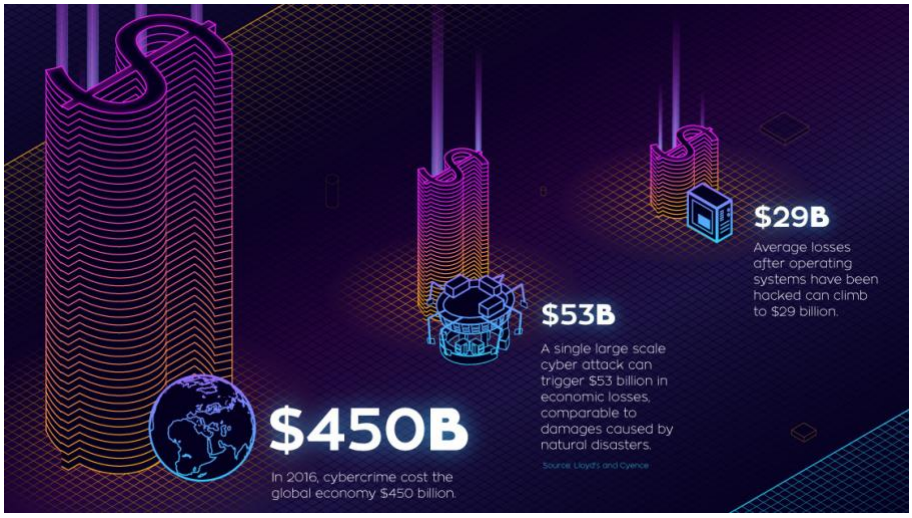
A key challenge that the world has faced regarding cyber security is what is generally dubbed the “Cyber Conflict”. This is the legal reflection based on the applicability of existing international law on activity on the internet. If the existing Hague conventions are deemed inapplicable to the internet then what other rules should be used? Is it time to create a new cohesive set of international online legal instruments? These are all subjects of controversial debate.

The second main challenge is based around the policy making infrastructure of many members of the alliance. The role and responsibility of the government in maintaining security online is highly disputed. Certain nations believe that the business sector should be responsible for maintaining public cyber security with many developed countries giving out contracts to firms to create security infrastructures. On the other side of the spectrum are countries that rely on the government to impose authority over the internet on a national level. There are even countries that suggest that the internet should be governed by inter-governmental organizations such as the International Telecommunications Union. This conflict was directly seen in the World Conference on International Communication in 2012 where there was a vote on an amendment to the International Telecommunication Regulation (ITR) which adds cybersecurity to the authority of the ITR. The US led coalition of 55 countries voted against the amendments, but they were outnumbered by the Russia and China led 85 country coalition in favor of the amendments to have a centralized regulatory body. A middle ground must be found regarding regulation and law in order to create a successful resolution on this topic. (“Centre for security development”)

While cyber-attacks have been around for many years, their mobilization on a larger scale military level is a relatively new development. Militaries have two main options for attack, syntactic and semantic attacks. These can be used as passive attacks or active attacks. A syntactic attack aims to disrupt or destroy a network by using various forms of sophisticated malware while semantic attacks aim to modify, steal or cover up information and data on a foreign network essentially aiming to corrupt important databases.

The main targets for these attacks have been on high importance infrastructures such as military and public control systems, Financial markets and databases and

telecommunication networks which generally have the largest impact on response functionality. After an attack, some basic analysis of losses and repairs are made the first of which is called a spectacularity review. In this review, specialists will calculate the total cost of losses suffered from the cyber attack. From this data and further analysis of the security infrastructure after the attack, a "Vulnerability Factor" is drafted. This is a figure that provides an overview on the general status of existing security systems and components, this allows for weaknesses to be identified and replaced. Many nations and companies will hire "White Hat" hackers to simulate an attack on their systems so that weaknesses can be identified before they are seriously exploited. NATO has various security programmes that use extensive aid from white hat hackers and security experts. The 2016 protocol for improving infrastructure had an advisory board of experts that suggested developments and analyzed existing. The success of a Communique depends on its ability to include expertise in this manner because it raises the quality of solutions. This inclusion of experts has been a relatively new development in NATO cyber security development solutions.



"Cyber Attacks Archives." Visual Capitalist, www.visualcapitalist.com/tag/cyber-attacks/.

Major Parties Involved

Russian Federation

The Russian Federation has been a figurehead player on the global stage when it comes to discussions to regulate and criminalize the abuse of advanced technologies since the late 90s. Furthermore, they have also adopted a highly influential role in different United Nations organizations. One example of which being the GGE (Governmental Group of Experts) along with a plethora of globalized institutions with the aim of regulating cyberspace on an international level such as the ITU (International Telecommunication Union). An example of this is how Russia presented a possible Code of conduct for securing information in cooperation with China in the year 2011, it took a highly regulatory stance but was particular about its proposals being government regulated by both internal and external organizations. Ideologically, Russia clearly has a very different approach to the issue of cyber security than the United States. While the US believes that it is important to preserve the free flow of data and information, Russia believes that too much free flow creates security vulnerabilities and weaknesses as networks become harder to scan and regulate. Russia has also been on the receiving end of cyber warfare. In the 2016 World Cup Russia managed to stop 25 million hack attempts into their infrastructural networks (“RT international”). On the other hand, they have been accused on multiple occasions of using cyber warfare with a primary example being in 2014 where a cyber weapon called Ouroboros was allegedly used by Russia to heavily disrupt Ukrainian government networks and functions. (“The Christian Science Monitor”)

China

Along with staggering economic growth due to an active manufacturing sector, China has become a global leader in internet use with more people connected to the internet than the populations of the US, Japan, Mexico and Russia combined (China Internet Network Information Center). This results in large amounts of data moving around on Chinese servers every day and thus China has deemed it necessary for the state to take a regulatory position over the internet before they lose control over online activities of the population. A key policy that indicates China's stance on the issue is the International Code of Conduct for Information Security that they proposed alongside the Russian Federation in 2011. A more domestic policy they recently implemented is the "China Internet Security Law" passed in 2017 which makes network operators store all data within China and allows the government to check any Chinese company's server and network data. The latter is what raised concerns over the technology company Huawei in the US as they believed that China was forcing companies to give them a backdoor to company and user data.

"China's Cybersecurity Law: An Intro for Foreign Businesses." China Briefing News, 11 Oct. 2018, www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/.

Turkey

Turkey adopts a similar policy structure to that of China. A NATO CCD review concluded that Turkey's security policy consists of 3 main ideas.

1. Ensuring the protection of all domestic transactions as well as all private and official databases and networks and doing so the entire domestic internet
2. Funding cyber security research and policy with the aim of decreasing the impact of cyber assaults on national systems and to have protocols that minimize downtime.
3. Making sure that the government has access to all national internet activity data from companies and individuals when it is pertinent to police investigations of matters of national security.

Turkey has recently unveiled plans to higher large amounts of white hat hackers and security experts to help develop its infrastructure to meet its goals of maintaining national information privacy and sovereignty. Turkish Cyber security cluster is one of these programmes.

"Global EPIC: Turkish Cyber Security Cluster Joins Expanding Global Innovation Initiative." Global, globalepic.org/item4349.

USA

The USA is one of the global leaders in technological development but also leads in the cyber security and surveillance field having many sophisticated programmes and weapons in its arsenal with an example being the xkeyscore web search that can track almost all internet user activity globally. They lead the world of intelligence gathering and processing both on a federal level with organizations such as the FBI and the US Cybersecurity Command but also on a private business level. The US has stated that they will only make use of their cyber weapons as a means of self defence but nations such as China have accused it of making use of almost 14000 Trojan viruses to target millions of Chinese servers. Edward Snowden's whistleblowing (Exposing secrets of a government or business) ordeal revealed a lot of key details about the massive extent of the US's cyber capabilities as well as suggesting that the US government has more authority over cyber space than what they have led the public to believe. The US have also used various cyber weapons to destroy Iran's military computer systems and destroying missile control networks as retaliation for allegedly attacking a US oil tanker.

Map showing live cases of cyber attacks worldwide as of 23/07/2019. You can use this interactive map which breaks down cyber-attacks on https://cybermap.kaspersky.com/.

Timeline of Key Events

Date - Description Of Event

1999 - First accounts of viruses being used with notable examples being the Melissa Email Worm

2000 - "ILOVEYOU" virus spreads rapidly and the US calls on the European Cybercrime treaty to create a more unilateral set of laws. First large scale use of Denial of Service tools in order to attack websites such as Yahoo, Amazon, CNN and eBay.

2001 - Widespread use of DoS attacks on government sites and public databases

2006 - NASA bans all emails with attachments in fear of them being hacked. Fears started after US space launch detailed had been hacked.

2007 - Conflict in Estonia over the removal of a Soviet war statue with Russia results in widespread denial of service attacks that destroy online banking and online government systems. Effects were reversed within days.

US department of Defense emails classified emails leaked by hackers and pentagon networks compromised.

China claims US and Taiwanese hackers stole information from Chinese networks and spyware was installed in the computers of officials.

2008 - Computers from US Republican and Democrat campaigns were hacked and data was extracted by unknown foreign intruders

Georgian computer systems were hacked during a period of high tension they

had with Russia. No real damage was done to cyber infrastructure

2009 - 5,000,000 computers launched a coordinated attack on Israeli internet networks. Israel claimed Hamas paid hackers in eastern europe to launch these attacks

2010 - A group going by the name of “Iranian Cyber Army” Hacks into Chinese search engines as well as Social media sites like Twitter. They used the hack to display Iranian propaganda messages

Stuxnet, a highly sophisticated cyber weapon is used against Iranian networks allegedly by the US to disrupt Iran’s nuclear programme

2011 - Large scale attack on Canadian government agencies by an unknown foreign source causes the Canadian central bank to go offline to protect data

24,000 files hacked into and stolen from the US department of defence

Russia and China propose Information security code of conduct

2012 - “Red October”virus discovered to have been stealing information from top level governments all around the world by using weaknesses in programmes such as Excel and Microsoft Word.

Television networks and financial service providers in South Korea were hacked and disrupted. They blamed North Korea

First ever meeting specialized on cyber defence set up by NATO hosted on June 4th. Promised to create a functional security infrastructure by october for all members. The programme was called the NCIRC (Nato Computer Incident Response Capability) and cost approximately 60 million euros. (“NATO Review”)

2013 - Indian hackers allegedly hacked into Pakistan's election databases and networks compromising highly sensitive data. Pakistani hackers responded by attacking over 1000 indian election databases

2014 - North korean hacking groups hack into Sony's networks and threaten violence and leaks if Sony releases their satirical comedy on Kim Jong-Un "The Interview"

2015 - After cyber attacks to US government networks. The US introduces a sanction plan for any individuals or groups found to be responsible for cyber crimes against the US with sanctions including the freezing of the hacker's assets.

2016 - NATO cyber defence pledge made to prioritize the development of cyber security infrastructures

2018 - Allies agree to set up a Cyberspace operations center in the Brussels Summit and allies agreed to give NATO security teams access to national security tools if needed.

Previous Attempts to solve the Issue

The most prominent international piece of legislation drafted to combat threats to cybersecurity was the Council of Europe Convention on Cybercrime or CEC for short. It is essentially an attempt at creating a unilateral legal approach and attitude towards cyber criminality. It made sure that members made the following online actions illegal:

1. Illegal Interception
2. Data Interference
3. System Interference
4. Illegal access
5. Misuse of electronic devices

It also made sure that members criminalized particular online activities such as Child pornography, Violations of trademarks/copyrights as well as fraud and forgery. A key criticism of the convention is that it allows states to pardon those who commit above crime without doing so with the intent of causing harm. This is highly vague language and certain legal systems will approach it differently than others meaning that the laws are not as unilateral as the CEC had hoped they would be.

The second most prevalent agreement is that of the Shanghai Cooperation organization or SOC for short. It was drafted with the help of leaders from Russia, Kazakhstan, China and several others in 2007. The treaty shares similar ideas as the when it comes to defining what participating nations should criminalize. However, the divergence between the two solutions appears when the SOC insists that nations use their governments as a regulatory body for cyber security in their countries. It also allows for the punishment of politically dissenting speech which would be a controversial policy with many NATO nations who list free speech as a right.

The International Telecommunications Union or ITU for short is another leading organization with the aim of defeating cyber crime. They are heavily cooperative with the UN General Assembly and hosted the World Summit on International Security where many nations urged the ITU to take a global leadership role in combating cyber warfare. This conference resulted in the creation of the Global Cybersecurity agenda which aims to assist nations in setting up cyber security infrastructures and creates partnerships between nations to assist each other

in improving their defenses and policies. The GCA has by far the most in depth understanding of tackling the issue from as many levels as possible with different approaches and departments for technical, political, economic, youth and institutional issues in the cyberspace. The united nations has also hosted many debates and assemblies in order to solve the issue however many nations continually fail to reach consensus on issues such as the applicability of humanitarian law to the internet and who has the authority to regulate the cyberspace.

Possible Solutions

There are many different ways of approaching the topic of cybersecurity. However there are certain key elements that can be more helpful to creating permanent solutions than others. These elements should be kept in mind when drafting amendments and solutions as well as during lobbying.

1. The involvement of cybersecurity expert organizations and institutions will be key to the success of any proposed solution. Some examples of organizations that could make for promising NATO cooperation are the ITU who already have extensive research on cyber attacks and have been able to get over 150 nations to sign their Global Cybersecurity Agenda which means that involving them into solutions will provide a headstart on consensus building between members as many would have signed onto the GCA already.
2. The analysis of previous large scale cyber attacks is key to understanding hacker behaviour and could help NATO understand the weaknesses of its members and be able to give better advice for the development of Firewalls and defenses. The challenge with this is that nations must be willing to share records of the attacks. Many members will not be willing to do so as they want to keep their defense structures private.
3. There is definitely a great disparity in the sophistication of cyberdefense infrastructures of different countries due to variations in economic development or how important internet connectivity is for a nation. There must be a clause that aims to help countries with weaker defenses to catch up. This can be done through

creating a NATO cybersecurity department advisory panel that can suggest improvements for cyber defenses. It is important that this disparity in defense quality is solved as the world is highly interconnected and a breach in one country can easily spill over to another.

4. A consensus must be reached on what kind of laws are to be used on the internet with particular attention to the application of international humanitarian law to cyberspace. This may not be a blanket policy, certain humanitarian laws may be easier to apply and regulate to the internet than others.
5. In order for any policies to be effective, nations must be able to agree on who has the authority to regulate internet activity. This could be NATO and its various departments or perhaps some kind of partnership with the ICC can be created. On the contrary, certain members may prefer to keep authority within their own borders and have their government dictate how information flows on the internet domestically. A middle ground could be that nations can have voting power on large scale decisions and verdicts on internet regulation.

Bibliography

EU and NATO Cyber Defence Cooperation - Parlementaire Monitor, www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk1h7j9gfuz2?ctx=vg9pj7ufwbwe&v=1&tab=1&start_tab0=580.

1803616372992612. “Quantum Computing - Can Blockchain Be Hacked?” *Hacker Noon*, Hacker Noon, 27 Feb. 2019, hackernoon.com/quantum-computing-can-blockchain-be-hacked-19c2ec7bac85.

“Cyberattack.” *Wikipedia*, Wikimedia Foundation, 20 June 2019, en.wikipedia.org/wiki/Cyberattack#cite_note-32.

“Cybersecurity - ICC - International Chamber of Commerce.” *ICC*, iccwbo.org/global-issues-trends/digital-growth/cybersecurity/.

"Glossary." *National Initiative for Cybersecurity Careers and Studies*, niccs.us-cert.gov/about-niccs/glossary#M.

Morgan, Jacob. "A Simple Explanation Of 'The Internet Of Things'." *Forbes*, Forbes Magazine, 20 Apr. 2017, www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#4df748731d09.

Nato. "Cyber Defence." *NATO*, www.nato.int/cps/en/natohq/topics_78170.htm.

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

Team, HostingFacts. "Internet Statistics & Facts (Including Mobile) for 2019." *HostingFacts.com*, 7 June 2019, hostingfacts.com/internet-facts-stats/.

"What Is Blockchain Technology? A Step-by-Step Guide For Beginners." *Blockgeeks*, 7 June 2019, blockgeeks.com/guides/what-is-blockchain-technology/.

Wyman, Oliver. "Global Cyber Terrorism Incidents on the Rise." *Marsh & McLennan Companies*, www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.