Committee: Disarmament and International Security

Issue: Towards unilateral cyber security measures against non-state actors

Student Officer: Nikolaos Artinos

Position: Chair

INTRODUCTION

In the last decade, cyber-attacks have been growing rapidly in scope and frequency across all nations. These attacks may soon be considered an "act of war"[1]. Countries like the United Kingdom, Russia, China, the United States of America, and Israel, have already implemented measures to combat cyberattacks that could possibly take place in the future. The term cybercrime is a general term used to cover computer-related offenses, content-related offenses, copyright-related offenses and most importantly, offenses against the confidentiality and integrity of personal data.

In the case of Non-State Actors, the impact of cyber-security threats may affect their economic status and may even affect valuable, important and classified information, which could possibly be extracted from them. Due to the increased number of cyber-attacks, nations (such as the United States of America) have developed tactics and methods to minimize the damage that can be caused by these attacks. Firstly, nations have tried and prevented cyber-attacks against critical infrastructure in a strategic way, in order to ultimately decrease the chances of a cyber-attack happening in the first place. This way, nations not only protect important and classified information, but they also protect non-state actors. The second precaution that nations take is reducing the national vulnerability to cyber-attacks by means such as: identification of threats, protection of valuable data, regular audit inspections, and risk assessments. Lastly, nations have also tried to minimize damage and recovery time from these cyber-attacks. With all these things to consider, it is only logical for governments to have made their cyber warfare capabilities an integral part of their long-term military strategy.

Implementing these strategies can be costly and time consuming, as there are multiple challenges to consider, such as the number of users, the availability of information, the missing mechanisms of control, international dimensions, automation, anonymous

[1] The History of Cyber Warfare - INFOGRAPHIC. (2019, January 30). Retrieved from https://online.lewisu.edu/mscs/resources/the-history-of-cyber-warfare

communication, and the encrypted technology that already exists. But aside from these general challenges, there are also legal ones, too. One common problem is that there are loopholes in the penal code, as no adjustments have been made to national laws that recognize the abuse of new technologies. This means, that it is difficult for international law to be adjusted constantly to the new forms of technology that are developed. With all these issues and challenges, we are left with a difficult question to face: Can Non-State Actors adapt to the challenges of cyber-security?

DEFINITION OF KEY TERMS

Cyberwarfare[2]

Cyberwarfare is computer- or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes.

Non-State Actor[3]

Non-state actors are individuals or organizations that have powerful economic, political or social power and are able to influence at a national and sometimes international level but do not belong to or allied themselves to any particular country or state.

Cybercrime[4]

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

Cybersecurity

[2] "What is cyberwarfare? - Definition from WhatIs.com." searchsecurity.techtarget.com/definition/cyberwarfare.

[3] "The Role of Non-state Actors in International Relations." www.academia.edu/5124220/The_Role_of_Non-state_Actors_in_International_Relations.

[4] "What is Cybercrime? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/2387/cybercrime.

Cybersecurity can be characterized as the act of the defence of an individual's or an entity's computers, private information, and other devices from cyber-attacks, which may involve theft or unauthorized utilization of data which may be private.

Hacking[5]

Hacking refers to unauthorized access into a computer or a network. A hacker may alter system or security features to accomplish a certain goal. Hacking can also refer to non-malicious activities such as unusual or improvised alterations to equipment or processes.

Cyberspace Operations[6]

The employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.

Cyberspace Superiority[7]

The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.

Data Protection

Data protection is the practice of ensuring the safety of private information from unauthorized use or loss.

Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot[8].

[5] "What is Hacking? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/26361/hacking.

[6] Maj Kha M, Nguyen. (2017). Adaptation to Hybrid Threats. Retrieved from https://web.archive.org/web/20161021143801/https://www.doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf

[7] Cyberspace Superiority. (n.d.). Retrieved from https://definedterm.com/cyberspace_superiority

[8] "Encryption." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 19 Dec. 2001, en.wikipedia.org/wiki/Encryption. Accessed 18 June 2019.

BACKGROUND INFORMATION

The Phenomena of Cybercrime

Development of the World Wide Web and cybercrime

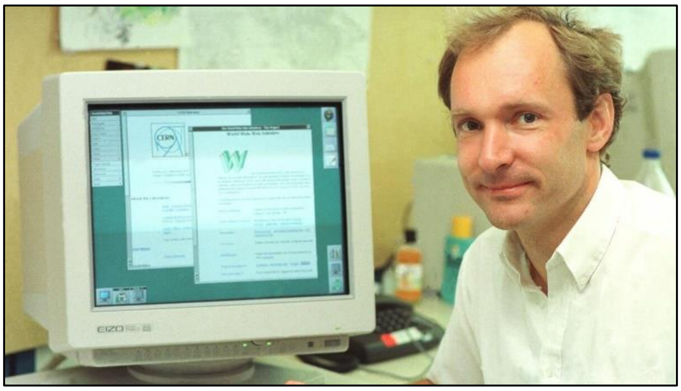

*Fig. SEQ Fig. * ARABIC 1 Tim Berners-Lee at CERN (1989)*

In 1989, Tim Berners-Lee invented the World Wide Web, which could be argued that since then has been the most important and greatest invention to be made. Since its creation, the World Wide Web has grown exponentially, and has offered unique services for everyone on a daily basis. The World Wide Web's growth has brought multiple positive changes to our lives. But its rapid growth has some disadvantages too, meaning that it has brought problems for humanity as well. This rapid growth has led to new forms of technologies being improved/formed constantly, and it has become harder and harder for governments to supervise them. Generally, cybersecurity threats, can be targeted towards organizations/governments or to specific individuals.

Impacts of cybercrime offences

In the 21st century, all sorts of new trends in cybercrime are being discovered constantly. Between 2000-2010, "botnet attacks" and "phishing" were the new methods of committing crimes on the World Wide Web. The damage caused by these attacks were devastating, as the emerging use of those methods were difficult for law enforcement to handle, tack down and investigate, which ultimately meant that they could not be supervised or dealt with effectively. The number of automated attacks increased significantly. This means that governments could not track the person/organization conducting them, which ultimately increased number of offences. These increased attacks have forced governments, organizations (and individuals) to respond to cybercrime with high priority. But throughout this study guide, we will be looking at the impacts, challenges and approaches to cybercrime for non-state actors specifically. Although these attack cyber-attacks take place multiple times per year, there is always a question to ask: What are the costs of cyber-attacks?

Generally, it is difficult to calculate the costs of cyber-attacks, as they are not representative of either the global development of cybercrime or of the true extent of cybercrime at the national level and are thus presented only to provide an insight into country information[9]. There are 2 main reasons so as to why costs are hard to calculate, and they are:

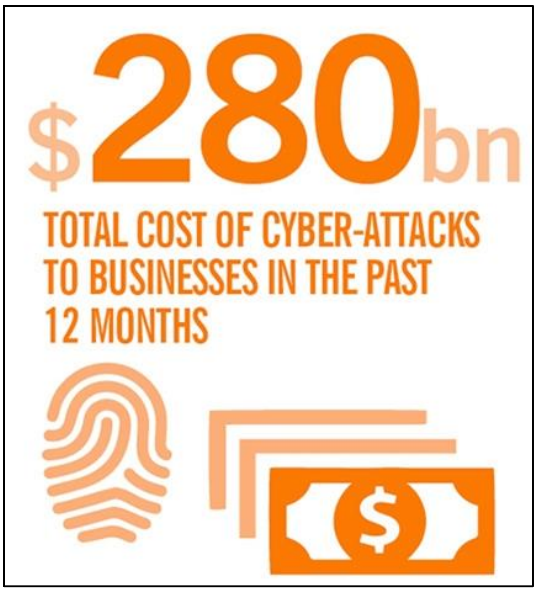
$280bn
TOTAL COST OF CYBER-ATTACKS TO BUSINESSES IN THE PAST 12 MONTHS
$

*Fig. SEQ Fig. * ARABIC 2 Global Costs of Cyber-Attacks in 2016*

1. Statistics are generated are at a national level, and not at an international level. This means that the generated values do not provide the holistic scope of the issue. This issue primarily exists because of variations in legislation that exist between nations, and the degree of compatibility between the data.
2. The generated cost value does not include cybercrime that has not been listed. This is common as cybercrime is sometimes undetected and not reported. Unreported cybercrime is one of the main issues and that is why it is difficult to calculate an overall cost, as breached businesses may have their image and reputation damaged if customers lose faith due to their vulnerability.

To put into perspective how expensive cyber-attacks are:

"The average cost of a data breach in the United States is $7.91 million USD" [10]

[9] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

[10] McCarthy, Niall. "The Average Cost Of A Data Breach Is Highest In The U.S. [Infographic]." *Forbes*, 13 July 2018, www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#63a735f72f37.

Fighting Cybercrime

Opportunities

There are several opportunities when it comes to fighting cybercrime. The 2 main opportunities are: Collecting Data Online and Automation.

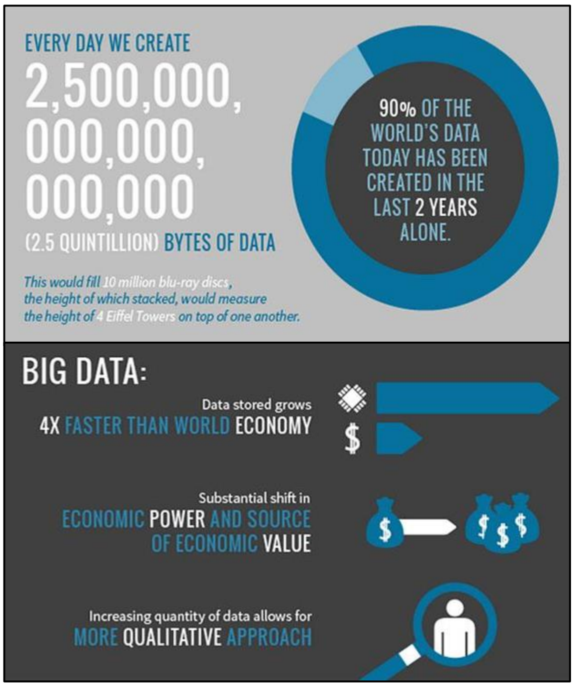

*Fig. SEQ Fig. * ARABIC 3 "The Characteristics of Big*

Collecting Data Online: Nowadays, numerous websites exist, and are used by hundreds of millions of users every single day. Some of these services are: Facebook, Instagram, Google, YouTube etc. In general, the business model of these popular websites is to track activities of their users. This is an opportunity for the government, as investigators can effectively carry out investigations and, for example, verify who the suspect communicated with prior to committing an offence[11]. With 2.5 Quintillion Bytes of Data (See fig 3) being generated every day, investigators have a lot of information to work with which can help indicate and evaluate sources of cybercrime. Data can not only help fight cybercrime, but it can also help fight physical crime. For example, the Los Angeles Police Department (LAPD) has collected data on more than 130 million crimes from the past 80 years which has helped them reduce crime by a substantial percentage. This has happened because there is a more holistic understanding of why crime occurs in certain areas[12]. But there can be a legal barrier for this opportunity, as businesses can sometimes refuse to give out information and data to investigators, as part of their policies for protecting consumers. Aside from the legal barrier, it can be costly and time consuming, and can be an opportunity cost for government.

[11] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

[12] "Big Data On The Internet – How Much Data Moves Around Each Day?" *Internet Marketing Strategies*, webbizkb.com/stats-and-tracking/big-data-on-the-internet-how-much-data-moves-around-each-day/.

Automation: In the past, searching for information on an alleged cyber-attack was carried out manually, which created a problem for investigator, as it was not an effective, quick, or low-cost method to discover relevant evidence. As mentioned previously, technology has improved exponentially over the past decade, which has helped investigators significantly. Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures[13]. While this may be an easier, quicker and more effective method for the gathering of evidence, the creation of software may be costly, and can have maintenance costs in order to remain up to date.

General challenges

While there are opportunities, what are the general challenges? The main challenges are: Speed of Development and Availability of Devices and Software, Number of Users, Encryption, Anonymous communications and International Dimensions.

Speed of Development and Availability of Devices and Software: With thousands of people joining the internet on a daily basis and quintillions of bytes being generated by users, the internet is undergoing development constantly. This means, that new challenges for law enforcement agencies are being posed all the time, which is extremely hard to deal with. But hardware devices are also developing rapidly. The latest home entertainment systems turn TVs into Internet access points, while more recent mobile handsets store data and connect to the Internet via wireless networks[14]. But in this day and age, criminals can commit serious offences with just second-hand computer technology. The date of production of the computer technology available has little influence on the use of that equipment to commit cybercrimes[15]. Cybercrime has also become more frequent, due to the fact that hackers are able to access and manipulate specialized software tools that are designed to crack passwords or to extract data. This ultimately means that investigators and agencies need to take the rapid development into account in order to make their work effective and successful.

[13] Giordano/Maciag, Cyber Forensics: "A Military Operations Perspective, International Journal of Digital Evidence", www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B.pdf

[14] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

[15] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

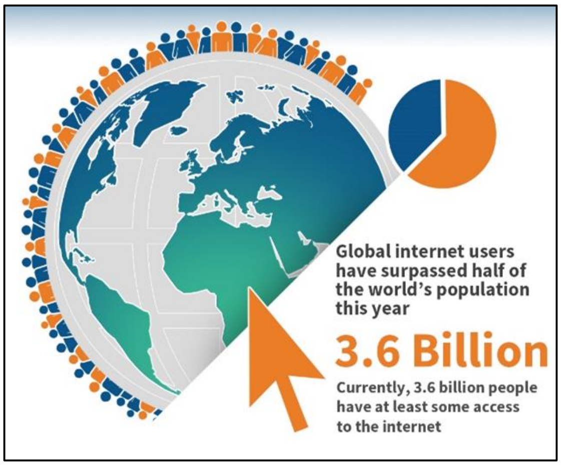
Global internet users have surpassed half of the world's population this year
3.6 Billion
Currently, 3.6 billion people have at least some access to the internet

*Fig. SEQ Fig. * ARABIC 4 Global Internet Users in 2018*

Number of Users: As discussed previously, the popularity of the internet is growing very rapidly, but this also means that the number of targets or offenders also increases. It is extremely difficult for governmental agencies to estimate how many people use the internet for illegal or immoral activities. Although Internet usage rates are lower in developing countries, promoting cybersecurity is not easier, as offenders can commit offences from around the world[16].

Anonymous communications: Determining the origin of communication is very often a key component of cybercrime investigation. However, the distributed nature of the network as well as the availability of certain Internet services, which create uncertainty as to origin, make it difficult to identify offenders[17]. This is because offenders have found multiple ways to hide their identities, which makes it hard for the government to a) track them down in the first place and b) identify them.

Encryption: Alongside anonymous communication, encrypted data can make the process of gathering evidence even harder. Encryption protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime[18]. As discussed previously, it is very easy for hackers to find specialized software tools that will encrypt data, and they can do it fast with just the click of the mouse. This means that investigators or law enforcement agencies may face encrypted material, which prevents them from gathering the needed information.

International Dimensions: The protocols for cybercrime differ drastically between nations. This means that if an offender is caught committing a cybercrime in different countries, investigations need the cooperation of law-enforcement agencies in all countries affected[19].

[16] "Phishing Activity Trends", *Report for the Month of April,* 2007www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[17] "Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence", Eoghan Casey,www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDEC80B5E5B306A85C4.pdf.

[18] "The CERT Division." *Software Engineering Institute*, 6 Nov. 2018, www.sei.cmu.edu/about/divisions/cert/index.cfm.

[19] Putnam, Tonya L. "International Responses to Cyber Crime." *Hoover Institution*, media.hoover.org/sites/default/files/documents/0817999825_35.pdf.

But this is difficult as it is difficult to operate on mutual legal principles across multiple nations and can be a large opportunity cost for the governments involved. Criminals may deliberately choose targets outside their own country and act from countries with inadequate cybercrime legislation[20]. This means that there needs to be effective cooperation between all nations, and harmonization of cybercrime-laws that exist between countries.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Group of Seven (Previously G8)

*Fig. SEQ Fig. * ARABIC 5 Group of 8, Lyon 1996*

In 1996, the Group of Eight (8), established a subgroup on High-Tech crime that aimed to deal with cybercrime. The Subgroup began with a mission to enhance the abilities of G8 countries to prevent, investigate, and prosecute crimes involving computers, networked communications and other new technologies[21]. Over time, the mission was expanded, and started to include work with Less Economically Developed Countries (LEDCs), on topics such as counterterrorism through the internet, and the protection of critical information. The main principles of this subgroup were:

1. *There must be no safe havens for those who abuse information technologies.*
2. *Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.*
3. *Law-enforcement personnel must be trained and equipped to address high-tech crimes.*[22]

[20] "Prepared Statement of the Federal Trade Commission On Efforts to Fight Fraud on the Internet." *Federal Trade Commission*, 30 Aug. 2013, www.ftc.gov/public-statements/2004/03/prepared-statement-federal-trade-commission-efforts-fight-fraud-internet.

[21] "G8 Subgroup on High-Tech Crime." *The IT Law Wiki*, itlaw.wikia.org/wiki/G8_Subgroup_on_High-Tech_Crime. Accessed 19 June 2019.

[22] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

United States of America

The United States of America has a vital role in the global fight for cybersecurity and has been trying to develop methods for effective cybersecurity in the past decade. Being confronted by multiple cyberattacks conducted by other nations, it is crucial for them to address the issue with high priority.

"The number of data breaches in the U.S. increased from 157 million in 2005 to 781 million in 2015, while the number of exposed records jumped from around 67 million to 169 million during the same time frame. In 2016, the number of data breaches in the United States amounted to 1093 with close to 36.6 million records exposed."[23]

*Fig. SEQ Fig. * ARABIC 6 US Department of Homeland Security Seal*

With cybercrime increasing exponentially, it is only logical for the government to have created, invested and subsidized specialized agencies that focus on cybersecurity and general investigations on cybercrime. One good example is the National Cyber Security Division (NCSD) which is essentially a division within the United States Department of Homeland Security. The NCSD was first formed on June 6, 2003, and had 2 overarching objectives:

"To build and maintain an effective national cyberspace response system.

To implement a cyber-risk management program for protection of critical infrastructure."[24]

Since its creation, the NCSD has increased the security of automated control systems that operate elements of the national critical infrastructure and has collaborated with the private sector and all sorts of stakeholders to increase cybersecurity and strengthen response and recovery methods. For further information on the United State's policies and strategies, you can click here to find out more.

China

While the Chinese government has been accused multiple times of conducting espionage on countries like Australia, Canada, the United States and India, it has taken steps

[23] "A Glance At The United States Cyber Security Laws." *Appknox | Mobile App Security, Resources, Best Practices & News*, 19 Oct. 2018, blog.appknox.com/united-states-cyber-security-laws/.

[24] "National Cyber Security Division." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 17 Dec. 2004, en.wikipedia.org/wiki/National_Cyber_Security_Division. Accessed 19 June 2019.

to strengthen its cybersecurity in the past decade. On 7th November, 2016, China created a new law which was named "Cyber Security Law of People's Republic of China", which aimed to increase cybersecurity and national security, protect the rights and interests of citizens and promote healthy economic and social development. The law essentially:

1. *Enhanced the principle of cyberspace sovereignty*
2. *Defined the security obligations of internet products and services providers*
3. *Detailed the internet service providers' security obligations*
4. *Perfected the rules of personal information protection*
5. *Established a security system for key information infrastructure*
6. *Instituted rules for the transnational transmission of data at critical information infrastructure* [25]

*Fig. SEQ Fig. * ARABIC 7 Cyber Security Law of the People's Republic of China*

Although the law faced some controversies, it has actually helped the Chinese Economy, as businesses have greater confidence, and are more willing to invest in certain projects such as Research and Development (R&D) in China.

Click here to find out more about China's Internet Security Law

Russian Federation

The Russian Federation has taken a different, more comprehensive and integrated approach to information security compared to Western Capital's focus on more technical network-centric cyber security[26]. Although Russia has focused extensively on the control of information, it has been affected by multiple cyberattacks, such as WannaCry (A ransomware attack that took in May 2017). Russia has previously stated that "uncontrolled information poses a threat to the government and society" and has shown a general interest in strengthening cybersecurity globally. Russia has partnered with China to develop the

[25] "China Internet Security Law." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 14 Apr. 2018, en.wikipedia.org/wiki/China_Internet_Security_Law. Accessed 19 June 2019.

[26] "Russia's Cyber Strategy." *ISPI*, 21 Dec. 2018, www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835.

International Code of Conduct for Information Security[27] and has also put forward multiple resolutions in the United Nations General Assembly.

TIMELINE OF EVENTS

Date	**Description of Event**
1982	The first ever U.S. cyberattack on a Soviet gas pipeline takes place, resulting in its explosion.
1989	Tim Berners-Lee invents the World Wide Web
1997	The G7 Establish a committee on High-Tech Crimes
2000	United Nation Convention Against Transnational Organized Crime – Palermo Convention
2000	The United Nations holds a conference on the Prevention of Crime and the Treatment of Offenders, which discussed computer related crimes.
2001	Convention on Cybercrime (Europe) – Budapest Convention
2004	The Convention on Cybercrime is created
2009	Creation of the Internet Governance Forum
2011	The Paris G20 summit suffered from a malware attack which gave access to hackers confidential G20 data.
2011	The Government of Canada suffers from cyber-attacks by foreign hackers.
2015	Germany Parliament Offices were compromised and internal data was uncovered.
2017	Ukraine Government Officials had malware on a Ukrainian tax website which spread the virus between other nations such as the United Kingdom, United States and France. Confidential information was lost.
2018	Northern Ireland Parliament Offices were hit by a brute force attack which gave hackers access to members' mailboxes.

[27] "Russia's Cyber Strategy." *ISPI*, 21 Dec. 2018, www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835.

2018	Facebook-Cambridge Analytica Scandal takes place, where theft of personal data from millions of users is stolen.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES, AND EVENTS

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

During the year 2000, a conference on the Prevention of Crime and Offenders was held in Vienna. At this conference, the impact of computer-related crimes was discussed, and generally the debate focused around categories of crime and transnational investigation, as well as a legal response to the phenomenon. Throughout the days of the workshop, capacity building and its importance were also highlighted. After this workshop, a conclusion was drawn, which stated: criminalization is required, legislation needs to include procedural instruments, international cooperation is crucial and public-private partnership should be strengthened[28].

Convention on Cybercrime

The convention on Cybercrime, or also known as the Budapest Convention, is the first international treaty seeking to address internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations[29]. The report produced by this committee, was adopted on 8 November, 2001. This convention had 3 main objectives, which were:

1. *Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime*
2. *Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form*
3. *Setting up a fast and effective regime of international cooperation*[30]

UN General Assembly Resolution 55/63

[28] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

[29] "Full List." *Treaty Office*, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[30] "Convention on Cybercrime." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 5 Aug. 2006, en.wikipedia.org/wiki/Convention_on_Cybercrime. Accessed 18 June 2019.

In the year 2000, the United Nations General Assembly adopted resolution 55/63, which was on combating the criminal misuse of information technologies. In this resolution, the United Nations successfully identified multiple measures that would ultimately enhance cyber-security for states. The resolution contained parts such as:

"States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies; Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States; Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies."

This resolution essentially encourages nations to take the required steps to ensure, maintain and improve cyber-security on a national level. This, of course, maybe by the development of domestic legislation to prevent criminal misuse of technologies and enhancing the ability to protect computer systems and data.

UN General Assembly Resolution 56/121

In 2002, the United Nations adopted resolution 56/121, which focused on the importance of cooperation among nations on combating the criminal misuse of information technologies. The resolution also emphasized how important the United Nations is in improving cyber-security, as well as the ways that it can assist. The resolution refers to the already implemented international approaches in fighting cybercrime[31].

"Noting the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime as well as the work of those organizations in promoting dialogue between the government and the private sector on safety and confidence in cyberspace"

Some major clauses of the resolution were:

1. Suggests that member States, when developing national law, policy, and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

[31] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

2. Takes note of the value of the measures set forth in its resolution 55/63, and again invites the Member States to take them into account in their efforts to combat the criminal misuse of information technologies;

3. Decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice"

UN General Assembly Resolution 57/239

Resolution number 57/239 once again deals with cyber-security, and essentially recalls resolution 56/121. This resolution emphasizes the importance of international cooperation in fighting cybercrime.

UN General Assembly Resolution 64/211

In March 2010, the United Nations General Assembly passed a new resolution as part of the "Creation of a global culture of cybersecurity" initiative[32]. This resolution deals with a major problem of cyber-security, namely the updating of legal authorities in order to improve and maintain cybersecurity. This resolution dealt with: cybercrime, commercial law, encryption, privacy, and data protection. Here are just 4 clauses that were mentioned in this resolution:

"13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

[32] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere."

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Global Protocol on Cybersecurity and Cybercrime

In 2009, the Internet Governance Forum was held in Egypt, where the issues surrounding cybercrime and cybersecurity were discussed, as well. The Internet Governance Forum (IGF) was established by the United Nations in 2006. The IGF is a prominent venue where civil society, industry, the technical community, and decision makers discuss key aspects of Internet governance issues on an equal footing[33]. Being a creation of the UN, it is also mandated by it as well. The IGF is run on a democratic bases, and deals with issues without the high intensity conflicts that characterize other international forums. During the forum that was held in Egypt, multiple things were discussed, such as: criminal law provisions, procedural law provisions, measures against terrorist misuse of the Internet, measures for global cooperation and exchange of information and measures on privacy and human rights[34]

*Fig. SEQ Fig. * ARABIC 8 The Internet Governance Forum's Logo*

Stanford Draft International Convention

In 1999, Stanford University in the United States hosted a conference similar to Europe's Convention on Cybercrime. Stanford approached cybercrime by developing a legal framework that would address all forms of cybercrime, which would ultimately strengthen

[33] "Internet Governance Forum." *Electronic Frontier Foundation*, www.eff.org/igf.

[34] Schjolberg, Stein. "A Global protocol om Cybersecurity and Cybercrime." *Cybercrime Law*, www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

cybersecurity across multiple nations. The conference mainly covered international cooperation, procedural law, and most importantly criminal law. The offences and procedural instruments developed by the Stanford Draft are only applicable with regard to attacks on information infrastructure and terrorist attacks, while the instruments related to procedural law and international law can also be applied with regard to traditional offences as well[35].

POSSIBLE SOLUTIONS

International Cooperation

The issue of cybersecurity threats is a vital one, and must be dealt with immediately, with effective and successful ways. Combatting cyber offences is extremely difficult, which means that all aspects of the problem must be addressed. As for the international and national legal frameworks in place, numerous measures must be taken in order to ensure that cybersecurity threats are regulated and do not threaten the sovereignty of nations. This can only be achieved through international cooperation. Nations need to assess their current cybersecurity laws and also define/look into their cybersecurity laws as well. But there needs to be a common ground, where nations can agree on the laws that other countries have, in order to prevent issues such as attacks being conducted by hackers that have moved to countries that have weak enforcement on cybersecurity laws. Countries are also expected to address any omissions or ambiguities in their laws that would enable evasion. Making cybercrime a global issue will not only spread awareness, but it will increase national efforts to improve or add to their legal framework for cybersecurity.

International investigations without the consent of authorities are extremely costly and difficult to conduct. Therefore, investigations need to be carried out with the support of the authorities in all the countries involved. Regarding the fact that in most cases there is only a very short time gap available in which successful investigations can take place, application of the classic mutual legal assistance regimes involves clear difficulties when it comes to cybercrime investigations[36]. In conclusion, improvement in international cooperation is a critical role in the improvement and development of cybersecurity strategies. Although it may

[35] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

[36] "Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

be difficult and time consuming to conduct, it will provide a safer environment to non-state actors in any country, which is extremely beneficial.

Capacity-Building and User Education

As discussed previously, cybercrime is a global phenomenon that needs to be dealt with immediately. With various challenges such as encryption, it is essential for laws to be harmonized with international cooperation. In order to ensure global standards in both the developed and the developing countries, capacity building is necessary[37].

But user education is just as important. Some cybercrimes, such as phishing (a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels[38]) do not depend on the technical aspect, but rather on the lack of awareness of users. Although there are some software tools that detect fraudulent websites, there is a limited accuracy, which means it cannot fully protect users. To solve this, user education is needed, which will ultimately reduce the number of potential targets. Workshops, lessons at schools and campaigns can be held in order to educate users. But to educate people effectively, there needs to be information on the latest cybercrime threats, and how they can be avoided or countered. All of this can be costly, but ultimately it will benefit the community, as cybercrime attacks will be reduced significantly.

International Cooperation

Due to the increased number of cybercrimes, there is bound to be an international dimension, due to the fact that there is no need for the physical presence of the attacker at the place where an attack is conducted[39]. The mobility of offenders, the independence from presence of the offender and the impact of the offence make it necessary for law-enforcement and judicial authorities to collaborate and assist the state that has assumed jurisdiction[40]. But achieving international cooperation can be difficult, as multiple differences in national laws and instruments that can be used to catch hackers exist. The first step would be looking into and assessing current cybersecurity laws internationally, and for countries to address any omissions or ambiguities in their laws that would permit evasion. International cooperation

[37] "The CERT Division." *Software Engineering Institute*, 6 Nov. 2018, www.sei.cmu.edu/about/divisions/cert/index.cfm.

[38] "What is Phishing? - Definition from WhatIs.com." *SearchSecurity*, searchsecurity.techtarget.com/definition/phishing.

[39] Sussman, Michale A. "The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium." *G7*,

[40] United Nations. "LEGISLATIVE GUIDES FOR THE IMPLEMENTATION OF THE UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOL THERETO."

may have administrative and logistical issues, but it will be beneficial, as ultimately it will significantly decrease cyber attacks on non-state actors and governments.

BIBLIOGRAPHY

"Costs of Cybercrime Have Soared to $280 Billion This Year." *Consultancy.uk | UK Consulting Industry Platform*, www.consultancy.uk/news/12917/costs-of-cybercrime-have-soared-to-280-billion-this-year.

"At the Abyss." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 25 Feb. 2019, en.wikipedia.org/wiki/At_the_Abyss. Accessed 19 June 2019.

"KPCB's Internet Trends 2016." *Advice Local*, 28 June 2016, www.advicelocal.com/blog/2016-internet-trends-report-infographic/internet-trends-2016-global-internet-users/.

"The Big Takeaways From the 2018 Internet Trends Report." *Advice Local*, 21 Aug. 2018, www.advicelocal.com/blog/2018-internet-trends-report/.

The History of Cyber Warfare - INFOGRAPHIC. (2019, January 30). Retrieved from https://online.lewisu.edu/mscs/resources/the-history-of-cyber-warfare

"The Role of Non-state Actors in International Relations." www.academia.edu/5124220/The_Role_of_Non-state_Actors_in_International_Relations.

"What is Cybercrime? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/2387/cybercrime.

"What is cyberwarfare? - Definition from WhatIs.com." searchsecurity.techtarget.com/definition/cyberwarfare.

"What is Hacking? - Definition from Techopedia." Techopedia.com, www.techopedia.com/definition/26361/hacking.

Maj Kha M, Nguyen. (2017). Adaptation to Hybrid Threats. Retrieved from https://web.archive.org/web/20161021143801/https://www.doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf

Cyberspace Superiority. (n.d.). Retrieved from https://definedterm.com/cyberspace_superiority

"Encryption." Wikipedia, the Free Encyclopedia, Wikimedia Foundation, Inc, 19 Dec. 2001, en.wikipedia.org/wiki/Encryption. Accessed 18 June 2019.

"Understanding cybercrime: Phenomena, challenges and legal response." Telecommunication Development Sector, www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf. Accessed 2014.

McCarthy, Niall. "The Average Cost Of A Data Breach Is Highest In The U.S. [Infographic]." Forbes, 13 July 2018, www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#63a735f72f37.

"Big Data On The Internet – How Much Data Moves Around Each Day?" *Internet Marketing Strategies*, webbizkb.com/stats-and-tracking/big-data-on-the-internet-how-much-data-moves-around-each-day/.

Giordano/Maciag, Cyber Forensics: "A Military Operations Perspective, International Journal of Digital Evidence",

www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B.pdf

"Phishing Activity Trends", Report for the Month of April, 2007www.antiphishing.org/reports/apwg_report_april_2007.pdf.

"Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence", Eoghan Casey,www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDEC80B5E5B306A85C4.pdf.

"The CERT Division." *Software Engineering Institute*, 6 Nov. 2018, www.sei.cmu.edu/about/divisions/cert/index.cfm.

Putnam, Tonya L. "International Responses to Cyber Crime." *Hoover Institution*, media.hoover.org/sites/default/files/documents/0817999825_35.pdf.

"Prepared Statement of the Federal Trade Commission On Efforts to Fight Fraud on the Internet." *Federal Trade Commission*, 30 Aug. 2013, www.ftc.gov/public-statements/2004/03/prepared-statement-federal-trade-commission-efforts-fight-fraud-internet.

"Full List." *Treaty Office*, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

"Convention on Cybercrime." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 5 Aug. 2006, en.wikipedia.org/wiki/Convention_on_Cybercrime. Accessed 18 June 2019.

"G8 Subgroup on High-Tech Crime." *The IT Law Wiki*, itlaw.wikia.org/wiki/G8_Subgroup_on_High-Tech_Crime. Accessed 19 June 2019.

"UofT G8 Information Centre: Lyon 1996." *G7 Information Centre*, www.g8.utoronto.ca/photos/summits/summit_photos_1996.html.

"A Glance At The United States Cyber Security Laws." *Appknox | Mobile App Security, Resources, Best Practices & News*, 19 Oct. 2018, blog.appknox.com/united-states-cyber-security-laws/.

"National Cyber Security Division." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 17 Dec. 2004, en.wikipedia.org/wiki/National_Cyber_Security_Division. Accessed 19 June 2019.

"China Internet Security Law." *Wikipedia, the Free Encyclopedia*, Wikimedia Foundation, Inc, 14 Apr. 2018, en.wikipedia.org/wiki/China_Internet_Security_Law. Accessed 19 June 2019.

"Internet Governance Forum." *Electronic Frontier Foundation*, www.eff.org/igf.

Schjolberg, Stein. "A Global protocol om Cybersecurity and Cybercrime." *Cybercrime Law*, www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

"The CERT Division." *Software Engineering Institute*, 6 Nov. 2018, www.sei.cmu.edu/about/divisions/cert/index.cfm.

"What is Phishing? - Definition from WhatIs.com." *SearchSecurity*, searchsecurity.techtarget.com/definition/phishing.

Sussman, Michale A. "The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium." *G7*,

United Nations. "LEGISLATIVE GUIDES FOR THE IMPLEMENTATION OF THE UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOL THERETO."