Committee: Disarmament and International Security Committee (GA1)

Issue: Addressing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats in international peace and security

Student Officer: Anna Kokla

Position: Deputy Chair

INTRODUCTION

In the recent years, technology has gained more and more power and, therefore, has become a major part of our everyday lives. It is true that technology rules the world. Undoubtedly, the Internet, the countless continuously updated electronic devices and the different forms of communication have shaped human interaction and have given a different meaning to it at all levels: social, political and cultural. Obviously, there are both positive and negative technological impacts on the world. However, this report will focus on one of the worst possible consequences of contemporary technologies: cyber threats and cyber terrorism. Cyber attacks, network security and information pose complex problems that reach into new areas for national security and public policy.

Cyber attacks are any kind of offensive actions through the Internet or computer networks conducted by individuals, nation-states, groups or organizations aiming at stealing, altering or even destroying a specific target by hacking into a susceptible system. They can range from installing spyware on a PC to malicious attempts to destroy the infrastructure of an entire nation.

Cyber attacks have become extremely sophisticated and complex due to the continuous technological progress that is taking place in the 21st century. As a result, their consequences are far more dangerous and obvious nowadays.

Therefore, the aim of the specific study guide is to provide the delegates with the needed information in order to enable them to carry out further research on this urgent topic that has a great impact on the prosperity of the modern world.

DEFINITION OF KEY TERMS

Cyber Threat

"The possibility of a malicious attempt to damage or disrupt a computer network or system."[1] As mentioned before, the targeted network can range from a PC to a nation-state network.

Cyber Terrorism

A common definition is very hard to be found. Nations do not seem to reach a consensus regarding the above term.

"Computer-based attacks aiming at disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population."[2]

"Terrorism conducted in cyberspace, where criminals attempt to disrupt computer or telecommunications service."[3]

Cyber Crime

"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 (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage."[4]

---

[1] English Oxford Learning Ditionaries. cyberthreat. n.d. web. 6 June 2017. <https://en.oxforddictionaries.com/definition/cyberthreat>.

[2] Dictionary. "cyberterrorism." n.d. web. 6 June 2017. <http://www.dictionary.com/browse/cyberterrorism>.

[3] Dictionary. "cyberterrorism." n.d. web. 6 June 2017. <http://www.dictionary.com/browse/cyberterrorism>.

[4] Technopedia. Cybercrime. n.d. web. 13 June 2017. <https://www.techopedia.com/definition/2387/cybercrime>.

Cyber War

"The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes."[5]

Phishing

Any attempt to obtain personal information or data, usually sensitive ones, such as passwords or credit card details, for malicious purposes.

Datum

The singular form of the word "data" is used to describe a single piece of information as a fact.

Denial of Service Attack (DoS)

"Any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service."[6]

Malware

"Software intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation."[7] Complex malwares are used

Worm

"A type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.[8]"

Figure 1: The detection of a virus in a PC

[5] English Oxford Living Dictionaries. "cyberwar." n.d. web. 6 June 2017. <https://en.oxforddictionaries.com/definition/cyberwar>.

[6] Technopedia. Denial-of-Service Attack (DoS). n.d. web. 11 June 2017. <https://www.techopedia.com/definition/24841/denial-of-service-attack-dos>.

[7] Dictionary.com. malware. n.d. web. 11 June 2017. <http://www.dictionary.com/browse/malware>.

[8] Technopedia. Worm. n.d. web. 11 June 2017. <https://www.techopedia.com/definition/4171/worm>.

Virus

"A type of malicious software (malware) comprised of small pieces of code attached to legitimate programs. When that program runs, the virus runs."[9]

Network

"A group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections."[10]

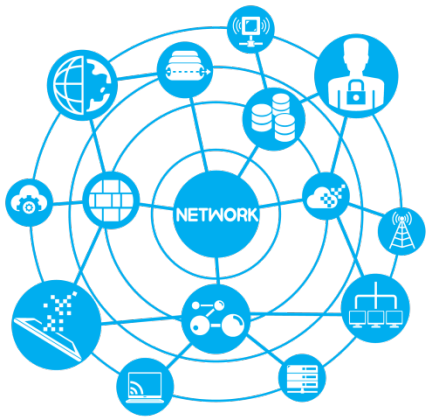

Figure 2: what a network consists of

Cyber Space

"The virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication."[11]

BACKGROUND INFORMATION

Cyber threats have existed since 1975 when Steve Jobs and Steve Wozniak invented the first personal computer. Then, many problems arose with hackers, people that strive to gain illegal access to personal information for either profit or to conduct mischievous acts.

The first cyber attack in history is known as the Morris Worm. The Morris Worm in 1988 spread around US computers, made the slow down to degree that they were unusable and, therefore, affected the world's cyber infrastructure.

In 1999, a teen hacks the NASA and the US Defense Department Networks, an action that changed a lot the perspective a lot of people had of cyber threats. The same year, the Melissa Virus would infect Microsoft Word documents and automatically disseminate itself as an attachment via an email. This email would be sent to the first 50 contacts in an infected computer's Outlook email address box. The creator of the specific malware did not intend to harm computers.

---

[9] Technopedia. Virus. n.d. web. 11 June 2017. <https://www.techopedia.com/definition/4157/virus>.

[10] Technopedia. Network. n.d. web. 12 June 2017. <https://www.techopedia.com/definition/5537/network>.

[11] Technopedia.Cyberspace. n.d. web. 13 June 2017. <https://www.techopedia.com/definition/2493/cyberspace>.

In 2009, Gonzales, a hacker form Miami, was responsible for one of the biggest fraud case in the US history. He managed to steal tens of millions of credit card and debit card numbers from over 250 financial institutions. He had hacked the payment card network of various companies.

In 2017, a new type of cyber attack has spread throughout 150 countries, including European states, as well as Australia. Hackers threaten the users to delete files and data unless a ransom is paid.

Types of Cyber Attacks

Malware

It is a malicious code with the aim of stealing data or destroying something on the targeted computer.

Phishing

Phishing attacks include emails that are sent to the targeted user and ask them to click on a link and enter personal data. That link directs the users to a specific site that will steal; the user's information. Those kind of attacks have got more and more complex and nowadays it is really difficult to distinguish a legitimate request for information from a false one.

Password Attacks

A third party tries to gain access to a system by cracking the password.

DoS Attack

As mentioned before, a Denial of Service attack focuses on overloading a network, thus, making it unable to function.

"Man in the Middle" (MITM)

By impersonating the endpoints in an online information exchange, the MITM can obtain information from the end user and the entity he or she is communicating with.

Drive-by Downloads

A program is downloaded to a user's system just by visiting the site. This takes place through malware. The downloaded program exploits vulnerabilities in the user's operating system.

Malvertising

Malicious code is downloaded to a computer when the user clicks on an affected ad.

Rogue Software

It is a malware that masquerades as legitimate and necessary security software that will keep the computer system safe.

Sources of Cyber Threats

Bot-Network operators

Bot-network operators are hackers. Instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate further attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets.

Criminal Groups

Criminal Groups seek to attack computer systems by using spam, phishing, and spyware/malware to commit theft and online fraud for monetary gain. International corporate spies and organized crime groups also pose a great threat to the US government because of their ability to conduct industrial espionage and monetary theft by developing hacker-talent.

Foreign Intelligence Services

Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. Several nations are currently working on the development of specific warfare programs, which have a significant impact on by disrupting the supply, communications and economic infrastructures that support military power. That could pose a great threat to the daily lives of the civilians.

Figure 3: a hacker breaking into a network

Hackers

"Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While hacking once required a fair amount of skill or computer knowledge, hackers can now

download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. The worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage."[12]

Insiders

Insiders may not possess a great deal of knowledge about computer intrusions, since their knowledge of a specific targeted computer system allows them to gain unrestricted access, in order to cause damage or to steal data. The insider threat also consists of employees who accidentally introduce malware into systems.

Phishers

"Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives."[13]

Spammers

Individuals or organizations, who distribute e-mails with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware or attack organizations.

Spyware/malware authors

Individuals or organizations with the intent to carry out attacks against users by producing and distributing spyware and malware. Several computer viruses and worms have harmed files and hard drives.

Terrorists

They seek to destroy, incapacitate or exploit critical infrastructures so as to threaten national security and cause major damage to the economy and the morale of the society.

The difference between cyber crime and cyber terrorism

When we talk about cybercrime and cyberterrorism, one of the underlying issues is the correct differentiation between the meanings of these terms. It is often a difficult task

[12,15] Industrial control Systems Cyber Emergency Response Team. Cyber Threat Source Descriptions. n.d. web. 6 June 2017. <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>.

to make a distinction between computer network attacks performed by terrorists and cyber-crimes done by hackers.

Cyber terrorism cases have a similar goal to real life terrorism cases: death and injury to human being physical destruction or damage to property, through the means of the Internet. As to the term cybercrime, it generally includes an illicit activity on the Internet as a whole.

Cyber attack consequences through a case study

In December 2016, Yahoo! reported two unprecedented cyber attacks, which were the biggest data breaches, involving the leaking of confidential data of more than a billion accounts. Nonetheless, the biggest issue that Yahoo has to deal with is not the loss of information or the direct damage to the server of the system, but several class action suits filed against it and the investigation by the Congress and the US authorities.

Yahoo's case illustrates the severe legal consequences that could occur as a result of a cyber attack in companies. They can be exposed to lawsuits from customers whose personal data have been compromised, from credit card companies and from companies with which they have confidential contracts.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

USA

Companies across the US are being increasingly targeted in cyber attacks since November 2014. The quantity and quality of information leaked, stolen or destroyed is one of the major issues that companies and individuals have to cope with. The Ponenom Institute release its 2015 Cost of cyber Crime, which analyses the cost of cyber attacks for a variety of 58 US organizations. Based on that research, the US continues to rank the highest in its cost of cyber crime at an annual average of $15.4 million per company. The US has also developed specific programs in order to tackle the problem of cyber threats. Some of them are the following:

- **Department of Homeland Security (DHS) Enhanced Cyber security Services (ECS) Program**, which is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their computer systems from unauthorized access, exploitation, or data exfiltration
- **Department of Defense (DoD) Defense Industrial Base (DIB) Cyber security (CS) Program,** which was initiated in 2007 and established as a permanent DoD program

in 2013 so as to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified networks or information systems.

- **DHS Cyber Information Sharing and Collaboration Program (CISCP),** which is a DHS's flagship program for public-private information sharing and complement ongoing DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.

China

Cyber attacks in Chinese companies have increased in the past two years. The average number of cyber attacks detected by companies in mainland China and Hong Kong grew 969 percent between 2014 and 2016. However, the average number of attacks fell by 3 percent globally over the last two years, and 30 percent since 2015, in contrast to the rise in China. China's rapid adoption of new consumer and industrial technology for the 'Internet of Things (IoT)' era may be part of the reason.

United Kingdom (UK)

Britain is being hit by dozens of cyber-attacks a month, including attempts by Russian state-sponsored hackers to steal defense and foreign policy secrets. Attacks by Russian and Chinese state-sponsored hackers on defense and foreign policy servers are among those being investigated by the National Cyber Security Centre (NCSC).

Russian Federation

In the past few years, the Russian government has mounted more than a dozen significant cyber attacks against foreign countries, to help or harm a specific political candidate and always to project Russian power. Starting in 2007, the Russians attacked former Soviet satellites like Estonia, Georgia, and Ukraine, and then branched out to Western nations like the U.S. and Germany.

Germany

Germany has been "cyber attacked" various times by Russia. The head of Germany's domestic intelligence agency has accused Russian rivals of gathering large amounts of political data in cyber attacks. However, the Russian government has denied such allegations.

Canada

Canadian companies are facing an increasing number of cyber attacks. Corporate espionage by state-sponsored hackers — including China — is a big problem for Canadian companies. That high increase in cyber attacks can be attributed to Canada's lack of trained cybersecurity professionals, since historically the country had not had the need to defend itself against other threats than its neighbors. However, Canadian government is currently moving in the right direction with a new legal requirement that firms disclose data breaches or any suspicious activity.

Australia

Australian companies are also facing increasing cyber attacks. Therefore, small companies are being urged to strengthen their cybersecurity measures. Recently, Australian businesses have likely been affected by the ransomware attack sweeping across Europe. So far the ransomware has wormed its way into thousands of computer systems worldwide shutting users out unless they pay a specific amount of money.

The National Cyber Investigative Joint Task Force (NCIJTF)

The National Cyber Investigative Joint Task Force (NCIJTF) is a Presidentially-mandated multiagency cyber center that coordinates, integrates, and shares information related to cyber threat investigations and operations. The NCIJTF currently has signed memoranda of understanding (MOUs) with approximately 24 member agency representatives, which allow for sharing of cyber threat information.

International Police (INTERPOL)

INTERPOL is committed to a global fight against cyber attacks and is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. Its plan consists of operational and investigative support, cyber intelligence and analysis, digital forensics, innovation and research, capacity building abnd National Cyber Reviews.

Federal Bureau of Investigation (FBI)

The FBI utilizes on-site briefings to share classified indicators and defensive measures with industry and appropriate private sector entities. Coordinating with its other government agency partners, it provides potential or known victim entities with temporary

security clearances so they may have access to specific classified information and technical indicators that may be used to neutralize an ongoing threat.[14]

National Cyber Security Centre (NCSC)

The NCSC was set up to help protect our critical services from cyber attacks, managing major incidents and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organizations. It is the UK's authority on cyber security.

North Atlantic Treaty Organization (NATO)

NATO and its Allies rely on strong and resilient cyber defenses in order to achieve collective defense, cooperation, crisis management and security. NATO signed a Technical Arrangement on cyber defense cooperation with the European Union (EU) in February 2016. Allies are committed to exchanging information and data related to dealing with and recovering from cyber attacks.

Information Sharing and Analysis Center (ISAC)

It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Its goal is to help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.

Cyber Security Task Force

The principal mission of the Cyber Security Task Force is to communicate information to American Bar Association (ABA) members in order to educate them and bring awareness to cyber security and privacy issues which they or their clients may encounter on a daily basis in the course of their legal practices.

International Multilateral Partnership Against Cyber Threats (IMPACT)

The IMPACT is a United Nations' (UN) specialized agency, which works with the goal of ensuring the safety of cyberspace for everyone. It is a key partner of the International

---

[14] The Office of the Director of National Intelligence. n.d.
. "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the CybersecurityInformation Sharing Act of 2015." 16 February 2016. web. 11 June 2017. <https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf>.

Telecommunication Union (ITU) has agreed to collaborate with other organizations in order to materialize ITU's Global Cybersecurity Agenda (GCA).

Commission of Crime Prevention and Criminal Justice

It was established by the Economic and Social Council in 1992 and its major goal is to improve international action towards combating national and transnational crime. It also provides states with a forum for exchanging expertise, experience and information in order to develop both national and international strategies to cope with criminal activities. Since cyber crime constitutes a crime itself, this organ of the United Nations (UN), responsible for combating crime, could collaborate with other NGOs with the goal of achieving cyber security.

TIMELINE OF EVENTS

Based on NATO's review of events[15], the timeline is as follows:

Date	Description of Event
1988	The Morris Worm was created and spread around computers in the US.
1995	Kevin Poulsen made sure that he would win the Porsche that KIIS FM was offering as he took control of the phone network and effectively blocked incoming calls to the radio station's number.
1999	Teen hacks NASA and US Defense Department. At the same time, the Melissa virus spreads through the Internet.
April 2007	Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial
June 2007	The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to

[15] NATO. Cyber Timeline. n.d. web. 10 June 2017. <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.

	access and exploit the Pentagon's networks.
January 2008	A New Jersey teenager along with a gang of hackers launched a DoS attack that crippled the Church of Scientology website for several days.
August 2008	Computer networks in Georgia were hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appeared on Georgian government websites.
2009	U.S. and South Korean government, financial and media websites are attacked, apparently by North Korea. Attacks targeting Twitter and Facebook succeed in taking both sites offline for several hours. Gonzales also manages steal tens of millions of credit card and debit card numbers from over 250 financial institutions by hacking the payment card network of various companies.
January 2010	A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message.
January 2011	The Canadian government reported a major cyber attack against its agencies, including Defense Research and Development Canada, a research agency for Canada's Department of National Defense.
October 2012	The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs.
June 2013	In their first-ever meeting dedicated to cyber defense on Tuesday (June 4), NATO Defense Ministers agreed that the Alliance's cyber-defense capability should be fully operational by the autumn, extending protection to all the networks owned and operated by the Alliance
October 2013	The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58 Million euro enhancement of NATO cyber defenses, is

	on track for completion by the end of October 2013.
2017	An unprecedented ransomware attack spread throughout 150 countries, including European countries, as well as Australia. Hackers threatening to delete files unless a ransom is paid.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

The following resolutions have been approved by the General Assembly.

- **A/RES/53/70**, Developments in the field of information and telecommunications in the context of international security, 4 January 1999

  This resolution was introduced in the General Assembly 1st Committee by the Russian Federation. It was adopted without a vote. It generally calls upon all states to realize the potential cyber threats, to collaborate with each other, as well as be willing to inform the Secretary General of their views of on the topic of information security.

- **A/RES/55/63**, Combating the criminal misuse of information technologies, 22 January 2001.

  This resolution tries to enforce already existing efforts of bodies relate to the topics as well as decides to be actively seized upon the matter of the misuses of information technologies.

- **A/RES/56/121**, Combating the criminal misuse of information technologies, 23 January 2002.

  This resolution takes into account and enforces the efforts of the Commission of Crime Prevention and Criminal Justice.

- **A/RES/57/239,** Creation of a global culture of cybersecurity, 31 January 2003.

  This resolution invites all member states to collaborate in order to develop a culture of cybersecurity, while bearing in mind the elements for creating such a culture. The specific elements are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.

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

  This resolution is actually a development of the previous one and, therefore, invites

member states and Non-Governmental Organizations (NGOs) to cooperate and take action.

- **A/RES/64/211,** Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17 March 2010.
  This resolution is similar to the previous ones; however the self-assessment tool is enforced.
- **A/RES/70/237,** Developments in the field of information and telecommunications in the context of international security, 30 December 2015.
  This resolution calls upon member states to take into consideration relevant reports submitted by the General Assembly.

What is more, since 2010, states like Germany, UK, the Netherlands, Sweden, Spain and Australia have submitted annual reports, which have been approved by the UN Secretary General, with their views on the issue *of "Developments in the field of information and telecommunications in the context of international security."* Such reports are:

- **A/65/154,** 20 July 2010
- **A/70/172**, 22 July 2015
- **A/71/172,** 19 July 2016

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

FBI Cyber Division

"The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are

Figure 4: The FBI Cyber Division

focused on cyber related matters."[16]

An Updated Draft of the Code of Conduct Distributed in the United Nations

On 9th January 2015, six members of the Shanghai Cooperation Organization (SCO) (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) proposed an updated version of the International Code of Conduct for Information Security to the United Nations. The document was submitted to the UN's Secretary-General Ban Ki-moon with a request that it be circulated as a formal document during the 69th session of the UN General Assembly. The previous draft of the Code of Conduct was submitted to the UN by China, Russia, Tajikistan and Uzbekistan in September 2011, which was not adopted by the UN, since it proposed too much censorship.

The updated draft takes into account the comments after the initial document was released and, therefore, there are some minor modifications, which do not change the essence of the Code.

Russia and U.S. Setup Cybersecurity Hotline to Prevent Accidental Cyberwar

During talks at the G-8 Summit in Enniskillen, Northern Ireland, the U.S. and Russia agreed to cooperate on a number of security issues, including improving communications about cyber threat data and cyber weaponry. The agreement focuses on increasing transparency between the two countries and reducing the possible instability or a crisis in their bilateral relationship. The leaders said that both governments would work together to create a mechanism for information sharing on hacking incidents and other cyber-attacks in order to better protect critical information systems.

The Budapest Convention on Cybercrime (2001)

It remains the most relevant international agreement on cybercrime and electronic evidence. Membership keeps growing, while both the quality of implementation and the level of cooperation between Parties keep improving. It provides States with:

- the criminalization of a list of attacks against and by means of computers;
- procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards;

[16] Monroe, Jana D. Testimony. 17 July 2003. web. 13 June 2017. <https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division>.

- International police and judicial cooperation on cybercrime and e-evidence.

  However, this Convention is not signed by all states and, therefore, is not applicable on a worldwide scale.

Cyber ShockWave

On February 16, 2010, a group of national security officials participated in a simulated cyber attack on the US, called Cyber ShockWave. This simulation provided an unprecedented look on how the government would respond to a large-scale cyber crisis. Unfortunately, the specific simulation showed that the US is not ready and does not have adequate policies in order to cope with potential cyber attacks.

POSSIBLE SOLUTIONS

The already adopted UN resolutions are too general to be correctly implemented, so delegates are invited to propose practical and detailed solutions.

Firstly, delegates should look into ways for all nations to establish global cooperation, strategies and policies aiming at combating cyber threats.

The creation of an international legal framework is of vital importance, since its absence creates instability, and, therefore, delegates should come up with ideas in order to tackle this challenge. The punishment of the perpetrators and the framework within which this should be done is also mandatory.

A consensus should be reached regarding a common definition of cyber terrorism. Since this seems to be utopian, delegates should discover the reasons why this is hard to achieve.

Raising the awareness of students, parents, educators, governments, small businesses on proactive and safety measures regarding cyberspace, as well as ways of recovering after a cyber attack has occurred is a great field of research. The contribution of the aforementioned NGOs and UN bodies involved is something that should not be omitted.

Cyber threats cannot be combated unless there is thorough research and adequate training of security officials or anyone related to the matter funded by certain institutions and donors. Therefore, delegates are asked to find such institutions, as well as ways to achieve the above.

At the same time, states should increase their security measures against cyber threats. Therefore, the already existing agencies and NGOs, which have been mentioned in

the “Major Countries and Organizations Involved” section (Sullivan), could be involved in that effort, support the governments and provide them with the adequate expertise.

The example of the USA is a great one and, thus, all states should be encouraged to conduct similar simulations on a regular basis, in order for the governments to be aware of any weakness concerning the immediate response against cyber attacks and be able to develop further mechanisms with the help of experts on the issue.

Concerning the Budapest Convention, delegates should come up with ideas, so as to provide the countries that remain outside the specific convention with incentives that will persuade them to do so.

Lastly, information sharing and transparency amongst the nations, as well as good monitoring of online practices by specialized agencies, like the FBI or the INTERPOL, in order to create an “Intelligence Pool”, can really act as a proactive measure against cyber threats.

BIBLIOGRAPHY

AAP and staff writers. Australian business hit by global cyber attack. 15 May 2017. web. 12 June 2017. <http://www.news.com.au/technology/online/hacking/australian-business-hit-by-global-cyber-attack/news-story/d723e2b5443bc0f739f55a37f86105e7>.

American Bar Association. Cybersecurity Task Force. 2016. web. 11 June 2017. <https://www.americanbar.org/groups/tort_trial_insurance_practice/cybersecurity_taskforce.html>.

ARM Staff. Top 10 most notorious cyber attacks in history. n.d. web. 10 June 2017. <https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/>.

Bipartisan Policy Center. "Cyber ShockWave." n.d. web. 13 June 2017. <https://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Final%20Cyber%20Brochure.pdf>.

Brownell, Claire. Cyber attacks on Canadian companies starting to ‘explode’, says president of cybersecurity firm. 9 May 2017. web. 12 June 2017. <http://business.financialpost.com/fp-tech-desk/cyber-attacks-on-canadian-companies-starting-to-explode-says-president-of-cybersecurity-firm>.

Catherine A. Theohary, John W. Rollins. "Cyberwarfare and Cyberterrorism: In Brief." 17 March 2015. web. 2 June 2017. <https://fas.org/sgp/crs/natsec/R43955.pdf>.

Cyber Threats: Definition & Types. n.d. web. 8 June 2017. <http://study.com/academy/lesson/cyber-threats-definition-types.html>.

Dictionary. "cyberterrorism." n.d. web. 6 June 2017. <http://www.dictionary.com/browse/cyberterrorism>.

Dictionary.com. malware. n.d. web. 11 June 2017. <http://www.dictionary.com/browse/malware>.

English Oxford Learning Ditionaries. cyberthreat. n.d. web. 6 June 2017. <https://en.oxforddictionaries.com/definition/cyberthreat>.

English Oxford Living Dictionaries. "cyberwar." n.d. web. 6 June 2017. <https://en.oxforddictionaries.com/definition/cyberwar>.

Global forum on Cyber Expertise. The Budapest Convention on Cybercrime: a framework for capacity building. 2016. web. 13 June 2017. <https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime>.

Grierson, Jamie. UK hit by 188 high-level cyber-attacks in three months. 12 February 2017. web. 11 June 2017. <https://www.theguardian.com/world/2017/feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin>.

IMPACT. Mission & Vision. 2015. web. 11 June 2017. <http://www.impact-alliance.org/aboutus/mission-&-vision.html>.

Industrial control Systems Cyber Emergency Response Team. Cyber Threat Source Descriptions. n.d. web. 6 June 2017. <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>.

InfoSec Institute. Cyberterrorism Defined (as distinct from “Cybercrime”). 21 December 2012. web. 13 June 2017. <http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/>.

International Telecommunication Union. UN Resolutions Related to Cybersecurity. 2017. web. 12 June 2017. <http://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx>.

INTERPOL. Cybercrime. n.d. web. 11 June 2017. <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>.

Jamie Grierson, Samuel Gibbs. NHS cyber-attack causing disruption one week after breach. 19 May 2017. web. 13 June 2017. <https://www.theguardian.com/society/2017/may/19/nhs-cyber-attack-ransomware-disruption-breach>.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: ." n.d. web. 2 June 2017. < https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf>.

Monroe, Jana D. Testimony. 17 July 2003. web. 13 June 2017. <https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division>.

National Council of ISACs. National Council of ISACs. 2016. web. 11 June 2017. <https://www.nationalisacs.org/>.

National Cyber Security Centre. About us. n.d. web. 11 June 2017. <https://www.ncsc.gov.uk/about-us>.

NATO Cooperative Cyber Defence Centre Of Excellence. An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New? 10 February 2015. web. 13 June 2017. <https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>.

NATO. Cyber defence. 17 February 2017. web. 11 June 2017. <http://www.nato.int/cps/en/natohq/topics_78170.htm>.
—. Cyber Timeline. n.d. web. 10 June 2017. <<http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.>.

NBC News. Chinses see almost 1000 percent increase in cyber attacks. 29 November 2016. web. 11 June 2017. <http://www.nbcnews.com/tech/tech-news/chinese-see-almost-1-000-percent-increase-cyber-attacks-n689466>.
—. Timeline: Ten Years of Russian Cyber Attacks on Other Nations. 18 December 2016. web. 11 June 2017. <http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>.
Rashid, Fahmida Y. Russia and U.S. Setup Cybersecurity Hotline to Prevent Accidental Cyberwar. 19 June 2013. web. 13 June 2017. <http://www.securityweek.com/russia-and-us-setup-cybersecurity-hotline-prevent-accidental-cyberwar>.

Shalal, Andrea. Germany challenges Russia over alleged cyber attacks. 5 May 2017. web. 11 June 2017. <https://www.itnews.com.au/news/germany-challenges-russia-over-alleged-cyber-attacks-460542>.
Sullivan, Megan. 8 Types of Cyber Attacks Your Business Needs to Avoid. n.d. web. 2 August 2017. <https://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/>.

Technopedia. Cybercrime. n.d. web. 13 June 2017. <https://www.techopedia.com/definition/2387/cybercrime>.
—. Cyberspace. n.d. web. 13 June 2017. <https://www.techopedia.com/definition/2493/cyberspace>.
—. Denial-of-Service Attack (DoS). n.d. web. 11 June 2017. <https://www.techopedia.com/definition/24841/denial-of-service-attack-dos>.
—. Network. n.d. web. 12 June 2017. <https://www.techopedia.com/definition/5537/network>.
—. Virus. n.d. web. 11 June 2017. <https://www.techopedia.com/definition/4157/virus>.
—. Worm. n.d. web. 11 June 2017. <https://www.techopedia.com/definition/4171/worm>.

The Office of the Director of National Intelligence. n.d.
—. "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the CybersecurityInformation Sharing Act of 2015." 16 February 2016. web. 11 June 2017. <https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf>.

United Nations Office for Disarmament Affairs. Developments in the field of information and telecommunications in the context of international security. n.d. web. 12 June 2017. <https://www.un.org/disarmament/topics/informationsecurity/>.

United Nations Office on Drugs and Crime. Commission of Crime Prevention and Criminal Justice. 2017. web. 1 June 2017. <http://www.unodc.org/unodc/commissions/CCPCJ/>.

Walters, Riley. Cyber Attacks on U.S. Companies Since November 2014. 18 November 2015. web. 11 June 2017. <http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014>.

Pictures' and Graphs' Bibliography

Figure 1: Separating Virus and Malware from Other Computer Problems. n.d. web. 18 June 2017. <http://www.chipandbytes.com/uncategorized/separating-malware-computer-problems/>.

Figure 2: Setting Up A New Business Network?Boomtown Makes it Easy. n.d. web. 18 June 2017. <http://www.goboomtown.com/additional-services/installations/network/>.

Figure 3: From Cashless to Moneyless: Inviting Hackers through Demonetization ! n.d. web. 18 June 2017. <http://techstory.in/hackers-demonetization/>.

Figure 4: FBI Cyber Division warns that the Aviation industry is under continual cyber-attack: GSN. n.d. web. 18 June 2017. <https://airportinformer.wordpress.com/2014/08/05/fbi-cyber-division-warns-that-the-aviation-industry-is-under-continual-cyber-attack-gsn/>.