Committee: Disarmament and International Security Committee (GA1)

Issue: Assessing and minimizing the risks of cyber attacks against States

Student Officer: Antonia Dalla

Position: Co-chair

INTRODUCTION

The use of technology has significantly increased the last few years, with internet and electronic devises being a major part of our lives. The countless continuously updated electronic devises, all the application that we use in our everyday lives and all the different types of communication that we have are some of the benefits of technology. But on the other hand, the progress of technology has led to the cyber attacks, a major problem in the modern society which affects individuals, companies and whole governments.

Cyber attacks are any kind of offensive actions through the Internet or any 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. Cyber attacks have become extremely sophisticated due to the technological progress of the 21st century. As a result, we have many different types of cyber attacks such as cyber threats, to a PC or to a nation-State system, cyber terrorism and cyber crimes (hacking, fishing, spamming) in which the cybercriminals are using their knowledge in order to find sensitive information of the victim or to find files for pornography or hate crimes.

Although, there are many types of cyber attacks and the problem is very big, this report will focus on the cyber attacks against the states, a phenomenon that threatens every nation who tries to develop its cyber security system and protect its information and data from the other nations.

The cyber attacks against states are leading to a war that is way different than the wars we have seen so far. The nature of the war has shifted from a physical war to an online war. This means that the soldiers will be replaced by hackers and the state governments try to find and damage the computers and information of the other nations. Such a cyber war not only can destroy states and support the traditional conflicts between the states but also cause serious tensions between the nations and may end to an actual war.

Therefore, this report will provide the delegates with the needed information about this issue but they should bear in mind that they should do their own research as well in order to find their countries policy on the topic and understand better the issue which is really crucial for the modern society and needs to be tackled.

DEFINITION OF KEY TERMS

Cyberwarfare

"Cyberwarfare is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems. Waged via the Internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services.

Cyberwarfare is also known as cyber warfare or cyber war."[1]

Cyber Terrorism

There is not a common about definition about Cyber Terrorism but the two definitions above describe the word better.

"The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society."[2]

"Computer-based attacks aimed at disabling vital computer systems so as to intimidate, coerce, or harm agovernment or section of the population."[3]

Cyber Threat

"The possibility of a malicious attempt to damage or disrupt a computer network or system."[4] And as it is mentioned before such treats can be to a PC or to a nation-state network.

[1]What Is Cyberwarfare (Cyber War)? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/13600/cyberwarfare.
[2]"Cyberterrorism | Definition of Cyberterrorism in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberterrorism.
[3]"Cyberterrorism."Dictionary.com, Dictionary.com, www.dictionary.com/browse/cyberterrorism?s=t.
[4]"Cyberthreat | Definition of Cyberthreat in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberthreat.

Network

"Is 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. The scale can range from a single PC sharing out basic peripherals to massive data centers located around the World, to the Internet itself. Regardless of scope, all networks allow computers and/or individuals to share information and resources."[5]

Cyberspace

"Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication."[6]

Malware

"Malware, or malicious software, is any program or file that is harmful to a computer user.These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission."[7]

Virus

"A computer virus is a small software program that can spread from one computer system to another and cause interferences with computer operations. A computer virus has the capacity to corrupt or to delete data on your computer and it can use an e-mail program to spread the virus to other email addresses in your online address book. In the worst case scenario, it can even delete everything on your hard disk"[8]

Cyber Espionage

---

[5]"What Is a Network? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/5537/network.
[6]"What Is Cyberspace? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/2493/cyberspace.
[7]"What Is Malware (Malicious Software)? - Definition from WhatIs.com." *SearchSecurity*, TechTarget, searchsecurity.techtarget.com/definition/malware.
[8]"Computer Virus." *One-Dimensional Dictionary Definition | One-Dimensional Defined*, www.yourdictionary.com/computer-virus.

"The practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."[9]

Cyber Weapon

"A piece of computer software or hardware used to commit cyberwarfare."[10]

Worm

"A worm is 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."[11]

BACKGROUND INFORMATION

The cyber warfare can be considered as less damaging than traditional warfare but this doesn't mean that type of warfare does not violate any articles of the UN charter or the International Law. Actually, cyber attacks violate the article 2.4 of the UN charter which states that: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[12] .The reason why this issue has not been solved is because cyber war is a relatively new conflict and the laws regarding the use of cyber weapons are still lacking.

Types of cyber attacks

The nation-states are using different types of cyber tools. Many of them are no different than the tools that are used for the cyber attacks against individual PCs.

---

[9]"What Is Cyber Espionage? | Cyber Espionage Definition." *Carbon Black*, www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.
[10]"Cyberweapon | Definition of Cyberweapon in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberweapon.
[11]"What Is Worm? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/4171/worm.
[12]"Chapter I." *United Nations*, United Nations, www.un.org/en/sections/un-charter/chapter-i/index.html.

DDoS attacks

A distributed denial-of-service (DDoS) attack is used to disrupt the nation-states communication systems. DDoS attacks are more popular becausean attacker can implement them with very limited resources against a larger, more powerful victim.

Malware

Viruses,worms and Trojan horses are popular tools that are used for the disruption of normal computer operations; they are secretly collecting data or destroying it completely. Such attacks are used because they are effective and fast and can collect the needed information.

Logic Bombs

Other kind of attacks are the Logic Bombs, which are malware that are designed to lie dormant until a specific time or until triggered by a certain event[13].With this type of malware the attack can't be perceived and the victim nation can't do something to neutralize it.

IP Spoofing

The attacker disguised himself and gain access to the private information without being perceived. Again, this type of attack has the advantage that the attacker can't be perceived and the victim state doesn't even know that has been attacked.

As it was mention before these types of attack are commonly used, even in home computers, but are still really catastrophic when they are used on a large scale by a warring nation-states.

Threats faced by the cyber attacks

Cyber attacks against states can cause all of problems to the victim state the most obvious is that the states lose their secret information and sensitive data are on the enemies' hands. But despite these obvious threats the victim state can face other threats that aren't so obvious and may be more catastrophically.

First of all, with all the cyber weapons that exist nowadays, a nation may not be aware of the fact that it has been attacked. This means that, through the cyber espionage, the nation which has targeted the victim nation will have sensitive information with ought

13

the victim state knowing it. So, the victim doesn't know that its data has been stolen or which data has been stolen so as to know the strategy that will follow after the attack.

Another threat is that the attackers, by using some malwares, can stole sensitive data or can cyber espionage a computer and remain anonymous. Or the cyber attack can be from a stolen computer, or from a computer of a cybercriminal that are paid to perform the attack. As a result the victim sate can't find who committed the cyber attack and in many times the real perpetrator can't be found.

Moreover, a cyberwarfare can be dangerous because of the potential of sabotage ormanipulate critical infrastructure of a country, as automated computer programs which canbe hacked, mainly run them. The consequences from a sabotage infrastructure could be catastrophic. For example a disabled electric grid or communications network would causechaos in a nation, disrupt its economy and prevent it from operating. Whilst this would result in a direct loss of life,over the long term such an attack could potentially be fatal.

Lastly, the speed and the origin of a cyber attack are unpredictable. The only thing is need for the attack is a computerand the knowledge, so the time and the date of the attack are impossible to be predicted. The fear of a big cyber attack is always a problem especially for the nations that aren't prepared to counter a cyber attack and they don't have the appropriate cyber security system.

The interests behind a cyber attack

Of course knowledge has power, so it is obvious that the motivation behind the cyber attacks is the information that the nation gains. The priority of the states is to collect the military and diplomatic information which are going to help them create the best strategy against the enemy nation. By knowing such information they have the advantage in negotiations and strategy decision as this information enables them to predict the possible strategic positions and decisions of the other state.

Moreover, they usually target businesses and companies and collecting information that are going to help them stand competitive against the world. Countries with strong and developed economies need the stolen trade secrets of their competitive nations and businesses in order to create strategies and plans that can make them rule the market and destroy the other nation's economy.

Lastly, the motivation behind some cyber attacks is to create damage to the state and paralyze basic infrastructure. This will make the victim state to give a lot of attention to the problems that are caused by the attack and this gives the advantage to the attacker state to committee other attacks against the state that are won't be perceived or to gain more economic and military power.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America

The USA has carried out many cyber attacks in the past. In 2007 US launched a worm against Iran in order to sabotage its nuclear program. But also has been targeted several times by governmental organizations and private companies in the past. The companies and the US government has to deal with many cyber attacks and information that has been leaked, stolen and destroyed. With all these attacks the US has developed a lot specific programs in order to tackle the problem of cyber attacks and cyber threats.

China

China is one of the states that use the cyber attacks in order to seek information and rule in the market. China targets many companies and obtains source code and sensitive data. It has become to super power to the cyberspace and has a lot of cyber weapons and this make China a major player in the digital era. The last two years, China's companies have been hit by several attacks.

Russian Federation

For the past years, the Russian government has carried out several cyber attacks against foreign states. Those attacks either had helped or had harmed a political candidate but always had protected the Russian power. Recently has been accused of planning to attack the US government agencies but it was discovered by Israel. In 2007, Russian started attacking to the former Soviet satellites like Ukraine, Estonia and Georgia and then moved to Western nations.

Germany

Germany is one of the western countries that Russia has targeted. The country has been cyber attacked many times by Russia and Germany has accused that the Russians are

gathering political data in cyber attacks but the Russian government has denied all the allegations.

United Kingdom

UK is being hit by several cyber attacks every month, including attempts from Russia and China to steal defense and foreign policy secrets. United Kingdom is the only cyber power in Europe, with the British government having invested heavily in cyber weapons the last few years.

Iran

Iran is another big player in cyberspace. Iran has developed its cyber capabilities and it seems that is behind several attacks. Iran has targeted the 5 cyber powers, United States, China, Russia, Israel and United Kingdom but especially the USA. And by knowing that attacks will result in reprisals, the Iranian hackers want to create damages to the victim States and they don't collect information.

Israel

Israel has a really developed cyber system with a lot of cyber weapons. It mainly operates with the United States, and has been blamed for one of the biggest attacks against the Iranian government. Also, Iran with USA has been accused for attacking many Western countries. Moreover, Israel was the state that discover that the Russians was planning to attack US government systems and after this discover, Israel hacked intoKaspersky Lab systems, a Russian software company.

North Korea

Although, North Korea's cyberwarfare capabilities are underrated, the country's name has been connected with some of the biggest attacks, including the Sony hack and the Bangladesh Bank heist. Also, the country has been linked with many other cyber attacks against states like South Korea, Japan and USA. In general North Korea is considered to be one of the states with the most powerful cyber force to launch an attack.

International Police (INTERPOL)

INTERPOL is a global coordination body which detects and prevents digital crimes. "Therefore, INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale.

Their main initiatives in cybercrime focus on:

- Operational and investigative support
- Cyber intelligence and analysis
- Digital forensics
- Innovation and research
- Capacity building
- National Cyber Reviews"[14]

National Cyber Investigative Joint Task Force(NCIJTF)

National Cyber Investigative Joint Task Force was established in 2008."As a unique multi-agency cyber center, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation."[15]

International Multilateral Partnership against Cyber Threats (IMPACT)

International Multilateral Partnership Against Cyber Threats is the first United Nations cybersecurity alliance and it is a specialized agency for ICTs,the International Telecommunication Union. IMPACT is the first partnership against cyber threats; it works as a platform that brings together governments and dealing with cyber threats. This partnership has 152 member countries and it is the largest cybersecurity alliance.

North Atlantic Treaty Organization (NATO)

"NATO and the European Union (EU) are cooperating through a Technical Arrangement on cyber defense that was signed in February 2016. In light of common challenges, NATO and the EU are strengthening their cooperation on cyber defense, notably in the areas of information exchange, training, research and exercises."[16]

TIMELINE OF EVENTS

This timeline will highlight some major cyber attacks and events that happened over the past two decades.

[14]https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[15]https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force
[16]NATO. "Cyber Defence." NATO, www.nato.int/cps/en/natohq/topics_78170.htm.

Date	Description of Event
1988	The Morris worm: It is the first recognized malware; the worm replicated itself in many computers especially in the United States. This worm has the intent to slow down the computers.
2007	The attack on Estonia's government: After the conflict between Russia and Estonia, the Estonia's government hit by several cyber attacks. Estonia responded well to the matter, and re-launched its online services within days after the attack.
2007	United States Secretary of Defense E-mail Hack:"The United States Deputy Secretary of Defense, during a speech about theDepartment of Defense's latest cyber security strategies, unveiled that a defensecontractor was intruded by unknown hackers, and about 24,000 files were stolenfrom the database of the Department of Defense."
2007	Attack on China's Ministry of State Security: China claims that various cyber attacks have targeted governmental and non-governmental organizations and hackers have collect data from key areas across China.
2008	US Presidential Elections Hack: "During the United State's presidential elections of 2008, both Republican andDemocratic parties were infiltrated. Unknown foreign intruders hacked andobtained all the data from both parties' networks and databases."
2008	Hack in Georgia: Computers in Georgia were hacked by unknown hackers while Georgia had a conflict with Russia. Offensive graffiti appeared on Government's website.
2009	Attack on Israel: Invaders hacked the state's internet infrastructure, causing its shut down acrossIsrael.
2009	Operation Aurora: China target cyber attacks against US companies
2011	Canada Cyber Attack: "An unknown external sourced hacked the Defense Research and Development Canada, which is a sub-research

	facility at the Canadian Department of National Defense. The government of Canada reported that the major cyber attack forced Figure 2-Cyber Warfare Targets the nation's most important financial agencies, the Treasury Board and the Finance Department, to go offline."
2011	US Department of Defense: The United States Deputy Secretary of Defense, during his speech unveiled that an unknown hacker stole 24,000 files from the database of the Department of Defense.
2012	Red October: "[17]In 2007, an international cyber attack began propagating through networks discreetly, without the knowledge and consent of any authoritative entity. Later in 2012, the Russian company Kaspersky discovered and identified the attack, and named it "Red October". Hackers involved with the attack successfully collected data via vulnerabilities and glitches in Microsoft Office's Word and Excel. The attack was aimed at nations in Eastern Europe, central Asia, and Russia. Traces of the invasion were later found in North America and Western Europe, after several reports about victims in the two regions. The malware gathered data from research agencies, military organizations, embassies, nuclear energy providers, and many other critical infrastructures."
2012	Flame attack: USA with Israel attack Iran and other countries in the Middle East.
2013	South Korea Attack: "North Korea is constantly carrying out attacks against its southern neighbor South Korea. In 2013, financial institutions in South Korea had their networks hacked by intruders in North Korea. In addition financial institutions, the most highlighted victimized institution were South Korea's broadcaster YTN."

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

These resolutions have been adopted by the UN 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 calls upon the states to realize the threats of the cyber attacks, cooperate with each other and also inform the Secretary General about their views on the topic.

- **A/RES/55/63**: Combating the criminal misuse of information technologies(22 January 2001)

  This resolution enforce the efforts of bodies relate to the topics and decides to be actively seized upon the matter of technology and information.

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

  This resolution takes into account 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 calls all the member states to collaborate in order to create a culture of cybersecurity and informs about the elements for creating such culture.

- **A/RES/58/199:** Creation of a global culture of cybersecurity andthe protection of critical information infrastructures(30 January 2004)

  This resolution is the development of the previous resolution and invites the member states and non- governmental organizations to 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 one.

- **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 all the member states to take into consideration reports submitted by the General Assembly related to the topic.

Budapest Convention on Cybercrime (2001)

This convention is the first international treaty that was signed on cyber crimes, via the internet and other networks. This treaty; addresses the cybercrime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

This issue is a really complex one and relatively new. And that why there are no previous attempts to solve it. Every nation tries to protect its networks and develop the strongest cybersecurity system. But we have some attempts from some nations and organizations which are trying to minimize the attacks or they are training their nation in order to develop their defense system against the attacks.

FBI Cyber Division

In response to the cyber crimes and the cyber attacks which have had devastating impact on the United States' economic and national security, FBI created Cyber Division in order to address cyber crime I a coordinated manner.56 Offices have been placed across the US staffed with agents who are there to protect the Nation and the citizens from cyber espionage, computer intrusions, theft of intellectual property and online fraud.

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 Russiaagreed to cooperate on a number of security issues, including improving communicationsabout cyber threat data and cyber weaponry. The agreement focuses on increasingtransparency between the two countries and reducing the possible instability or a crisis intheir bilateral relationship. The leaders said that both governments would work together tocreate a mechanism for information sharing on hacking incidents and other cyber-attacks inorder to better protect critical information systems."

Cyber ShockWave

On February 16, 2010, a group of former senior administration and national security officials simulated a cyber attack against the United States. This simulation had the purpose to show how the United States would respond to a large-scale cyber attack that would affect much the nation. Unfortunately, this simulation shown that USA was not ready for such a big attack. However, this experiment proves the importance of cybersecurity for a nation and how hard is to have a developed and strong cybersecurity system.

POSSIBLE SOLUTIONS

This topic is one of the most challenging issues in the modern society. The already existing resolutions are general and they don't solve this important issue. For these reasons the delegates need to find creative and effective clauses that are going to tackle the problem and minimize the cyber attacks against the states.

First of all, the delegates must find ways to strengthen the already existing law about cyberspace and also the creation of a legal framework, which will create stability; are mandatory. The punishment of the predators and the framework which this should be done is of vital importance.

Moreover, the cooperation between all the member states in order to create strategies and policies against the cyber threats is another solution. At the same time, the states should develop and empower their cybersecurity systems and find new security measures against the cyber attacks. So they need to cooperate with NGO's and special agencies in order to achieve something like that.

Additionally, the example of USA is a great one, and all the members should follow this example and frequently simulate possible attacks to their nations in order to find the lacks of their defense system and with the help of experts on the issue, improve and develop further mechanisms.

Lastly, the delegates should find ways to persuade the states that aren't members of the Budapest Convention to join. And also, the creation of a data base in which the states are going to share information about cyber attacks that they have faced or new cybersecurity systems that have beencreated could be a solution.

BIBLIOGRAPHY

"Computer Virus." *One-Dimensional Dictionary Definition | One-Dimensional Defined*, www.yourdictionary.com/computer-virus.

"What Is Cyber Espionage? | Cyber Espionage Definition." *Carbon Black*, www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.

"Cyberweapon | Definition of Cyberweapon in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberweapon.

"What Is Worm? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/4171/worm.

"Chapter I." *United Nations*, United Nations, www.un.org/en/sections/un-charter/chapter-i/index.html.

"Cyberthreat | Definition of Cyberthreat in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberthreat.

"What Is a Network? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/5537/network.

"What Is Cyberspace? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/2493/cyberspace.

"What Is Malware (Malicious Software)? - Definition from WhatIs.com." *SearchSecurity*, TechTarget, searchsecurity.techtarget.com/definition/malware.

What Is Cyberwarfare (Cyber War)? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/13600/cyberwarfare.

"Cyberterrorism | Definition of Cyberterrorism in English by Oxford Dictionaries." *Oxford Dictionaries | English*, Oxford Dictionaries, en.oxforddictionaries.com/definition/cyberterrorism.

"Cyberterrorism."Dictionary.com, Dictionary.com, www.dictionary.com/browse/cyberterrorism?s=t.

"Arms Control Today."*Nonproliferation Benefits of India Deal Remain Elusive | Arms Control Association*, www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.

Breene, Keith. "Who Are the Cyberwar Superpowers?" *World Economic Forum*, www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

"Full List."*Council of Europe*, Council of Europe, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Greenberg, Andy. "The Iran Nuclear Deal's Unraveling Raises Fears of Cyberattacks."*Wired*, Conde Nast, 9 May 2018, www.wired.com/story/iran-nuclear-deal-cyberattacks/.

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

Skroupa, Christopher P. "Cyber Warfare -- Reasons Why Israel Leads The Charge." *Forbes*, Forbes Magazine, 7 Sept. 2017, www.forbes.com/sites/christopherskroupa/2017/09/07/cyber-warfare-reasons-why-israel-leads-the-charge/.

Volz, Dustin. "U.S. Charges, Sanctions Iranians for Global Cyber Attacks on Behalf..." *Reuters*, Thomson Reuters, 24 Mar. 2018, www.reuters.com/article/us-usa-cyber-iran/u-s-charges-sanctions-iranians-for-global-cyber-attacks-on-behalf-of-tehran-idUSKBN1GZ22K.

"What Is NATO?" *NATO*, www.nato.int/nato-welcome/index.html.

Wagner, Daniel. "The Growing Threat of Cyber-Attacks on Critical Infrastructure." *The Huffington Post*, TheHuffingtonPost.com, 25 May 2017,

www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html?guccounter=1.

"Nation State Cyber-Attacks on the Rise - Detect Lateral Movement Quickly." *SC Media UK*, www.scmagazineuk.com/nation-state-cyber-attacks-rise-detect-lateral-movement-quickly/article/1473191.

"Reducing the Threat of State-to-State Cyber Attack against Critical Infrastructure through International Norms and Agreements." *Center for International Security Studies at Maryland*, 1 Dec. 2010, www.cissm.umd.edu/publications/reducing-threat-state-state-cyber-attack-against-critical-infrastructure-through-0.

"Action against Cybercrime." *Council of Europe*, Council of Europe, www.coe.int/en/web/cybercrime/home.