Committee: Special Political and Decolonization Committee (GA4)

Issue: The development of cyber peacekeeping

Student Officer: Angelica Vogiatzoglou

Position: Chair

INTRODUCTION

In the modern world that we live in technology is exponentially developing. In the past decades there has been undoubtedly a significant internet evolution. Technology and the cyber space have provided us with immense opportunities. However, technology has also posed many threats and risks to our society. Henceforth, the international community should not lay back and has to strive to ensure that collective and immediate action is carried out for all cyber threats to be eradicated and for data to be effectively protected.

With a rapid development in technology, cyber security issues are becoming an everyday struggle affecting individuals, companies and governments. According to an Online Trust Alliance (OTA) report[1], in 2017 the number of cyber attacks doubled and reached 160,000, with ransomware attacks in the lead. In 2018 and 2019, apart from ransomware, cryptomining was significantly used by cybercriminals. The evident vulnerability of the internet, the rise in cyber-attacks and recent incidents are some of the reasons why it is crucial that the issue of cyber warfare is dealt with now.

Cyber warfare is a wider term to describe all attacks between nations and international organizations with the use of computer technology to disrupt each other's privacy and security. Some types of cyber warfare are espionage, sabotage, propaganda, data breaches, Denial of Service (DoS). The international community should be aware that all political and military disputes is also mirrored in cyberspace. The rapid and unpredictable advancement of technology means that the cyberspace conflicts could be as or even more detrimental than attacks happening on the ground. Leon Panetta, a former US Secretary of State and former director of the CIA, in October 2012 mentioned that: "A cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the

[1] *Cyber Incident & Breach Trends Report*. Online Trust Alliance, 2018, *Cyber Incident & Breach Trends Report*, www.internetsociety.org/wp-content/uploads/2019/04/2018-cyber-incident-report.pdf.

terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation. ”[2]

There is significant internet vulnerability and inadequate cyber protection. This is where cyber peacekeeping needs to step in. Cyber peacekeeping is a very promising and innovative way to restore peace in cyberspace and aims at protecting civilians, increasing trust and cyber protection, preventing cyber conflicts but also mitigating their consequences and rebuilding infrastructures after the cyber conflict. Cyber peacekeeping should definitely be used to prevent and combat cyber threats.

DEFINITION OF KEY TERMS

Peacekeeping

Collins English dictionary defines peacekeeping as “A peacekeeping force is a group of soldiers that is sent to a country where there is war or fighting, in order to try to prevent more violence. Peacekeeping forces are usually made up of troops from several different countries”[3]

UN Peacekeepers are sent to post-conflict zones in order to help torn nations rehabilitate and rebuild peace. Other than maintaining security and peace, UN peacekeeping operations restore political processes and order, oversee disarmament and protect human rights. However, the aim of this study guide is not to focus on peacekeeping itself but on how peacekeeping actions could be translated into cyber peacekeeping.

Cyberspace

Merriam Webster Dictionary defines cyberspace as:”the online world of computer networks and especially the Internet”[4]

Cyber Peacekeeping

Although cyber peacekeeping refers to peacekeeping actions taking place in cyberspace, no detailed, universal definition has been found. Cyber peacekeeping could be defined as operations which maintain peace and security in cyberspace after cyber conflicts and cyber crimes have been paused. The cyber peacekeepers would implement agreements,

[2] “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.” *United States Department of Defense*, 11 Oct. 2012, archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[3] “Peacekeeping Definition and Meaning | Collins English Dictionary.” *Peacekeeping Definition and Meaning | Collins English Dictionary*, www.collinsdictionary.com/dictionary/english/peacekeeping.

[4] “Cyberspace.” *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/cyberspace.

be engaged as mediators before a conflict, bring an end to and respond to the conflict and restore peace, security and infrastructure in the torn cyber region.

Cyber warfare

Cyber warfare or Cyber war is any virtual conflict which uses the internet to attack a country's computers incited by political and strategic means with the aim of attacking and sabotaging the opponent's information systems, damaging communication and transportation systems, water and electricity supplies through viruses and denial of service attacks.

BACKGROUND INFORMATION

History of cyber warfare

The Morris worm is the first recognized attack which affected the world's cyber infrastructure. Robert Tappan Morris was a graduate student who wanted to figure out how big the internet was. Thus, in 1988 he created a program which travelled from computer to computer and sent back signals to the server. However, the program created a worm, without Morris realizing it. It overloaded and completely blocked computers. This was the first incident of distributed denial of service attack. Since then, cyber attacks have become a reality. Especially now, with the exponential development of the internet, cyber attacks are becoming an even more regular phenomenon.

Other important cyber attacks were the denial of service attack towards the Estonian government in 2007 following a disagreement with Russia. In January 2009, Israel's governmental computer system was hacked during a military confrontation in the Gaza Strip. In 2010, Stuxnet was the first cyber weapon designed to cause physical harm; it reportedly aimed at destroying the Iranian nuclear weapons. In 2014, cyber attacks from Russia against Ukraine were reported during the seizure of Crimea by pro-Russian rebel groups and during the Ukrainian elections. In 2015, there were also alleged cyber attacks from Russia and China towards Germany and the United States of America, respectively. In 2017, WannaCry ransomware attacks were reported. It is believed to have affected more than 200,000 computers which used Microsoft Windows in more than 150 countries. In 2017, NotPetya weaponized ransomware struck as well. NotPetya originated in Ukraine; it destroyed files and the damage it created was huge.

Types of cyber attacks

Multiple cyber threats exist. Some of them are espionage, sabotage, propaganda and denial of service.

Espionage

Espionage, in other words spying, is the process of obtaining secret information regarding the plans and activities of a nation, an individual or a company. The spies or, in the case of cyber espionage, the hackers, obtain military, political, commercial and other information without the holder's consent. In cyber space, espionage is undertaken through the illegal monitoring of devices. The cyber criminals that carry out cyber espionage in case of low cyber security could shut down governmental infrastructures and obtain confidential information. Such cyber attacks have changed election results and made companies succeed or fail.

North Korea, China, Vietnam and the USA are considered nations which are masters in cyber espionage. In 2019, cyber espionage attacks from Iran and China against the USA have been reported. It is widely believed that they are the result of the USA withdrawal from the Iran nuclear deal. In 2018, a Chinese-sponsored 12-year cyber espionage campaign was revealed. Intelligence agencies from Beijing were aiming to steal trade secrets and other intellectual property from approximately 13 nations, including the USA.

Sabotage

Cyber sabotage is a continuously growing and imminent threat. It is defined as the deliberate disruption of the normal functions and the destruction of equipment or information.

A clear example of a cyber sabotage attack is the one carried out in 2012 against the Saudi Arabian oil and gas company "Aramco", one of the biggest oil companies in the world. 350,000 computers were partially or totally disrupted and destroyed. The exports of the company were paused for 2 weeks. Thus, the financial and commercial consequences were huge for the oil company. A Stuxnet attack in 2010 was also a sabotage cyber attack.

Propaganda

Cyber Propaganda can be defined as the deliberate effort to manipulate information and alter public opinion towards a certain point of view. Cyber propaganda regularly follows on after database hacking, espionage and data breaching. Certain information is stolen and it is revealed strategically in order to create a negative impact. Cyber propaganda is also perpetrated through fake news. Fake news is the spreading of false information again with the objective of altering public opinion. Fake news could change instantly viewpoints and is generally considered a strong tactic. In the 2016 US president election, false headlines and fake news published in Facebook outperformed real news.

Tools of cyber attacks

In order for cyber attacks to be undertaken, some tools are necessary. Identifying these tools and finding ways to encounter them is crucial for the handling of cyber attacks.

Ransomware

Ransomware is a type of malware which does not allow users to open their files. From the moment the malware affects a device, it asks users to pay in order for them to access their personal files. Nowadays, ransomware authors most times ask payment to be sent via cryptocurrency. Ransomware authors use messages to trick people to download files or click on links. Notpetya and WannaCry attacks are some of the latest cyber attacks based on ransomware.

Denial of Service (DoS)/ Distributed Denial of service (DDoS)

Denial of Service is an effort to block users from gaining access to a device or a network. Denial of Service is achieved by overloading a network and hindering the legitimate requests from being completed. The difference a distributed denial of service has is that system flooding comes from many different sources. The Morris worm and Estonian 2007 cyber attacks are some clear examples of denial of service attacks.

Goals, roles and functions of cyber peacekeepers

In order for all these cyber attacks to be encountered, organized cyber peacekeeping actions need to be carried out. In this section we will examine the goals, roles and functions of cyber peacekeepers before a conflict, during a conflict and after it.

Cyber peacekeepers have some very important and specified goals. They have to protect civilians, prevent and mitigate conflicts, implement trust and security and help torn parties rehabilitate. Cyber peacekeepers should restore peace, trust, security, organization and rebuild political structures.

The roles of cyber peacekeepers would be certain and critical. Cyber peacekeepers would act as arbitrators and mediators before conflicts, as guardians and “builders” when it comes to the aftermath of the conflict.

The functions of the cyber peacekeepers are different before the conflict, during the conflict and after it. Before a cyber attack the cyber peacekeepers would carry out Research and Development in order to identify potential cyber threats. They would also reinforce the capacity and capabilities of networks and devices. In this way, cyber protection would be very high. Cyber peacekeepers would also arbitrate between parties of potential cyber conflicts. Concerning the functions of cyber peacekeepers during the cyber conflict, they would assist in ceasing the conflict, stopping its spread, mitigating its consequences and responding to it. After the conflict, cyber peacekeepers would help torn governmental infrastructures, devices or networks stabilize and recover. They would also examine the containment of information and devices in order to ensure that such offences are prevented in the future.

Henceforth, we conclude that cyber peacekeeping deals with cyber conflict, attacks prevention, de-escalation, mitigation, aftermath containment and rebuilding.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America (USA)

In the USA, cyber war is part of its military strategy. The USA claims that a cyber attack directed at its nation would be considered casus belli. The USA has both perpetrated and been the target of some cyber threats. Officials like Leon Panetta have pointed out the importance and dangerousness of cyber attacks and conflicts. The USA cyber peace and cyber counterintelligence forces are also in development. On April 2009, the US Department of Defense announced that it had spent more than $ 100 million on the repair and reaction to cyber attacks. In 2007, when the cyber attack in Estonia hit, NATO set up the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn for the better cyber research and development and defense in the region. In 2016, the Obama administration, before leaving office, assigned $19 billion for research and development on cyber security.

Russia

It has been reported that Russia has carried out multiple cyber attacks against other nations and has been accused of many major cyber attacks. It undertook the 2007 attack against Estonia, the 2015 cyber attack against TV5Monde, the Paris-based broadcasting service (all of whose 12 channels were almost destroyed by Russian hackers) , the 2008 attacks against Georgia, the 2015 attacks against Germany and the cyber attacks against Ukraine in 2014 to disrupt the Ukrainian presidential elections. It has been reported that Russian hackers have interfered both in the 2016 US presidential elections and in the 2016 UK referendum regarding the exit of the United Kingdom from the European Union. Russia has claimed that it has carried out some denial of service attacks as a part of their defense strategy. In recent years, Russia seems to profoundly use cyber attacks in its security strategy. Russia has developed great computational power in comparison to other countries and this makes Russia particularly strong in the sector of cyber defense.

North Korea (DPRK)

North Korea is reported to possess more than 6,000 hackers who carry out attacks in order to raise money for the country's nuclear program. DPRK has been accused of carrying out cyber attacks against South Korea, Vietnam, Japan and some Middle East countries. DPRK has also been accused of undertaking attacks against Sony Pictures in 2014. DPRK was also accused of the major WannaCry cyber attack in 2017.

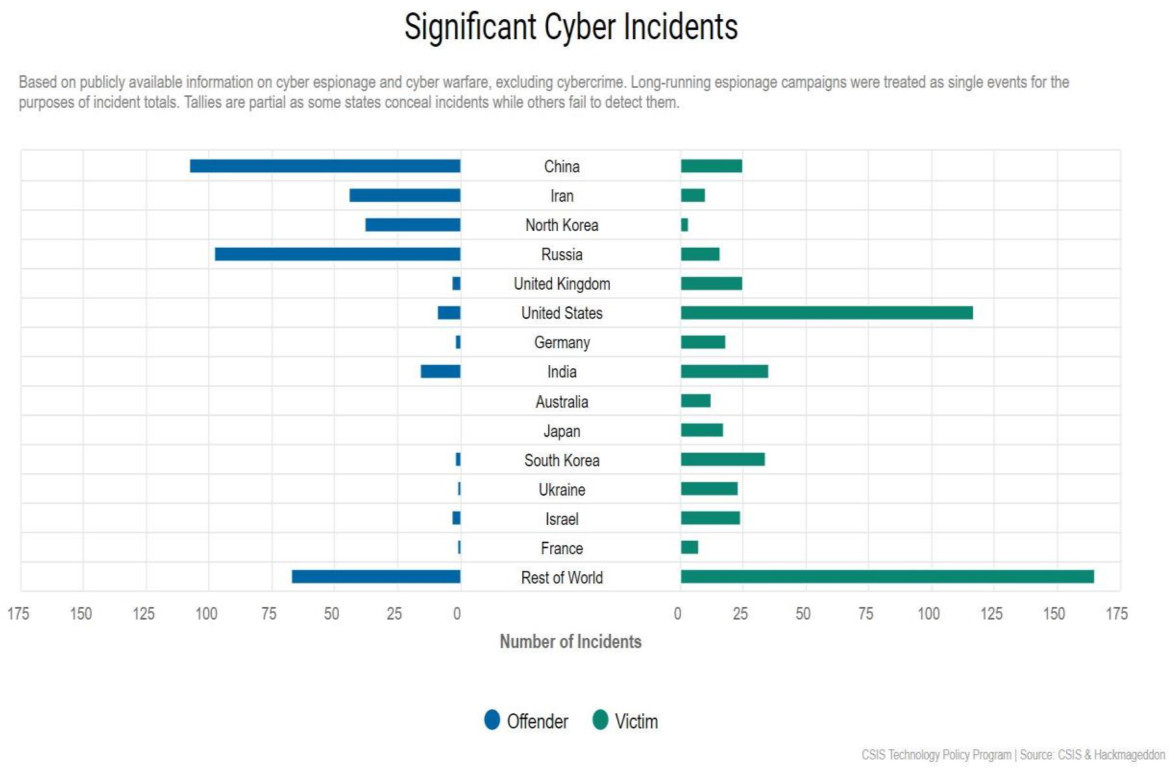

Figure 1: Graph which focuses on major cyber attacks since 2006 and whether some countries were victims or offenders, source: "Significant Cyber Incidents." *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

TIMELINE OF EVENTS

Date	Description of Event
1950	The term of peacekeeping was coined
1988	The first cyber attack which affected the global infrastructure, the Morris Worm cyber attack took place.
1994	The Chechnya cyber propaganda conflict between pro-Chechen and pro-Russian forces took place. They had a virtual war by posting false information about each other, which created public confusion, after their conflict on the ground.
1999	After the bombing of Serbia by NATO, pro-Serbian hackers started attacking the NATO information systems. NATO, US and UK computers were all attacked during the conflict.
2007	The detrimental attack from Russia towards Estonia was carried out. The attack targeted the Estonian government, banking and media.
May 14, 2008	The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) was established by Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain.
2010	Stuxnet cyber attack struck.
March 2014	Russia carried out a Denial of Service attack against Ukraine
May 2014	Russia carried out a cyber attack against Ukraine and influenced the Ukrainian presidential elections.
June 2015	Chinese hackers stole 21.5 million data records from the US Office of Personnel Management
December 2016	Another Russian backed cyber attack against Ukraine took place.
May 2017	WannaCry ransomware struck.
June 2017	NotPetya ransomware attack struck.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

- UN Digital blue helmets (DBH) and Sustainable Development Goals (SDGs)

The United Nations has established the Digital Blue Helmets (DBH) initiative. This organ is regarded as cyber peacekeepers. They carry out extensive research and development based on cyber threats and the impact they could have on the UN. They have also shaped a cyber peacekeeping policy and they want to ensure better coordination of cyber peacekeeping measures. As a cyber security component, the digital blue helmets initiative has shaped and adjusted some of the Sustainable Development Goals (SDGs) to cyber potential. The Digital Blue Helmets could be described as a very promising and effective initiative.

- United Nations Institute for Training and Research (UNITAR)

The United Nations Institute for Training and Research (UNITAR) has also organized a panel and discussions on cyber security in order for the cyber threats to be well known and researched in order for the UN to develop well organized Cyber peacekeeping.

- UN GA Resolutions

In January 2002, the GA resolution 56/121 was voted upon which focused on cyber crimes and on combating the criminal misuse of information technologies. In January 2003, Resolution 57/239 was also voted upon which focused on the global culture of cyber security.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

There have been some previous attempts to solve the issue of cyber attacks. Research on new technologies and cyber defense, development of more resilient information systems and cooperation between countries has been carried out. However, most of them have not been that effective, taking into consideration the fact that cyber attacks are still on the rise. Apart from UN initiatives, there have also been cyber peacekeeping initiatives from other organizations. However, the issue is still a novel one and more cyber peacekeeping actions need to be carried out.

In July 1, 2004 , the Council of Europe voted upon and adopted the Budapest Convention, in other words, the Convention on Cybercrime. It has 63 State Parties. Some non-Council States signed the convention, as well. However, it has not achieved unanimous global support yet due to the fact that opposing policies still exist. The convention was the first international treaty on cyber crimes and focused on pornography and network violations. This convention aims at achieving international cooperation and legislation.

Apart from the Council of Europe, NATO has also strived, more successfully, to solve the issue of cyber attacks. On May 14, 2008, following the Estonian 2007 cyber attacks, Estonia along with six other nations established the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). The CCDCOE has organized conferences and carried out research on technology, legal issues and cyber defense strategies. It is responsible for the training and education in cyber defense for all NATO members. By 2019, the NATO Cooperative Cyber Defense Center of Excellence has grown to 25 members. The CCDCOE has carried out many important actions for cyber defense strategy and more nations should be encouraged to participate in and contribute to the organization's initiatives. The CCDCOE organizes the annual International Conference on Cyber Conflict, "CyCon", in which 600 experts participate and deal with cyber defense issues in an interdisciplinary manner. The CCDCOE has also been carrying out an annual cyber defense exercise called "Locked Shields" since 2010 in order to help countries limit their information systems' vulnerability. Lastly, the CCDCOE has published the most comprehensive guide, the Tallinn Manual 2.0 on how international law applies to cyber attacks and defense strategies in today's world.

POSSIBLE SOLUTIONS

The issue of cyber security and cyber peacekeeping is a relatively new one. Although cyber attacks and cyber threats have existed since the 1980s, cyber peacekeeping is an innovative issue which is right now under discussion and debate. What is certain is that global policies have to be formed in order for cyber peacekeeping actions to be developed and monitored. Cyber threats are on the rise and immediate cyber peacekeeping actions need to be deployed.

Firstly, the committee could propose to the Security Council the formation of a council which would monitor actions in cyberspace in order to ensure that international and transnational agreements and human rights are not violated. The action of Digital Blue Helmets should be further supported and developed. All UN member States should work towards this objective.

Furthermore, some changes in the structure of networks and databases could also seem very helpful in order to avoid major cyber attacks and detrimental consequences. More specifically, when a network is centralized and has only a central server, then, if this server is hacked, the virus will affect the whole network. If this structure is altered to a decentralized and distributed database, then the attacks would only affect one of the computers of the network and not all of them. Decentralized and distributed network means that it possesses no central administrator and information is not only stored in one computer but in all participating computers of the network.

Moreover, Disarmament, Demobilization and Reintegration activities carried out by peacekeepers should be translated into cyberspace and such actions should also be carried out by cyber peacekeepers. Cyber peacekeepers should also have the appropriate capacity and capabilities to perform their roles and functions and achieve their goal before, during and after a cyber conflict.

Lastly, training and digital education as well as the raising of awareness about cyber threats have to be carried out. Not only should the public be informed about the significance of emerging technologies and the internet, but also about its threat and how someone can detect a threat and protect themselves.

BIBLIOGRAPHY

Akatyev, Nikolay & James, Joshua I. (2015). Cyber Peacekeeping. 126-139. 10.1007/978-3-319-25512-5_10.

“9 Latest Cyber-Espionage Affairs | EC-Council Official Blog.” *EC*, 8 Mar. 2019, www.blog.eccouncil.org/9-latest-cyber-espionage-affairs/

“A Brief History of Cyberwarfare.” *GRA Quantum*, 6 Dec. 2018, www.graquantum.com/a-brief-history-of-cyberwarfare/

“Activities | Digital Blue Helmets.” *United Nations*, United Nations, www.unite.un.org/digitalbluehelmets/activities.

Britannica, The Editors of Encyclopaedia. “Espionage.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 5 June 2017, www.britannica.com/topic/espionage

“Budapest Convention and Related Standards.” *Cybercrime*, www.coe.int/en/web/cybercrime/the-budapest-convention.

“Budapest Convention and Related Standards.” *Cybercrime*, www.coe.int/en/web/cybercrime/the-budapest-convention.

Cyber Incident & Breach Trends Report. Online Trust Alliance, 2018, *Cyber Incident & Breach Trends Report*, www.internetsociety.org/wp-content/uploads/2019/04/2018-cyber-incident-report.pdf.

"Cyber Sabotage." *Military.com*, 6 Feb. 2008, www.military.com/defensetech/2008/02/06/cyber-sabotage.

"CYBER WARFARE | Meaning in the Cambridge English Dictionary." *Cambridge Dictionary*, www.dictionary.cambridge.org/dictionary/english/cyber-warfare.

"Cyber Warfare." *RAND Corporation*, www.rand.org/topics/cyber-warfare.html.

"Cyberspace." *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/cyberspace.

Fruhlinger, Josh. "Cybersecurity Facts, Figures and Statistics for 2018." *CSO Online*, CSO, 10 Oct. 2018, www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

Geers, Kenneth. *Cyberspace and the Changing Nature of Warfare* . NATO, *Cyberspace and the Changing Nature of Warfare* , www.ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf.

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

"Peacekeeping Definition and Meaning | Collins English Dictionary." *Peacekeeping Definition and Meaning | Collins English Dictionary*, www.collinsdictionary.com/dictionary/english/peacekeeping.

"Ransomware - What Is It & How To Remove It." *Malwarebytes*, www.malwarebytes.com/ransomware/.

“Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.” *United States Department of Defense*, 11 Oct. 2012, www.archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Robinson, Michael, et al. *An Introduction to Cyber Peacekeeping*. De Montfort University, 2018, *An Introduction to Cyber Peacekeeping*, www.dora.dmu.ac.uk/xmlui/bitstream/handle/2086/16097/introduction-cyber-peacekeeping-accepted.pdf?sequence=1&isAllowed=y

Shackelford, Scott, and Indiana University. “What the World's First Cyber Attack Taught Us about Cybersecurity.” *World Economic Forum*, www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges

“Significant Cyber Incidents.” *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Tara Seals US/North America News. “Cyberattacks Doubled in 2017.” *Infosecurity Magazine*, 26 Jan. 2018, www.infosecurity-magazine.com/news/cyberattacks-doubled-in-2017/

“The inside Story of the Biggest Hack in History.” *CNNMoney*, Cable News Network, www.money.cnn.com/2015/08/05/technology/aramco-hack/index.html

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

“What Is Peacekeeping .” *United Nations*, United Nations, www.peacekeeping.un.org/en/what-is-peacekeeping

“The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub.” CCDCOE, www.ccdcoe.org/