United Nations Security Council

Combatting the Sabotage of Key Infrastructure Using Cyberspace

Research Report

Leiden Model United Nations 2021

The power of the Internet

Forum:	*United Nations Security Council (UNSC)*
Issue:	*Combatting the Sabotage of Key Infrastructure Using Cyberspace*
Student Officer:	*Derin Kalkan, Joanna Mavromati*
Position:	*President, Deputy President*

Introduction

The Internet, being one of the most significant breakthroughs in the history of technological advancement, fosters innovation and has completely shifted our interaction patterns. Our reliance on digital technology has affected our society, culture and now plays a key role in politics and transnational matters. However, it serves as a point of vulnerability which can be easily exploited by malicious actors. Cyberspace has introduced a new space where terrorist organizations, politicians and large corporations can go untraced, expand their agendas and achieve their goals through manners which were previously unimaginable. Moreover, cyberspace is a rather new and unexplored area, making illegal actions taken in it difficult to identify. To add to that, cyberweapons, such as viruses and malicious software, are distinctly more demanding to trace than physical weapons since they are digital and often leave no footprint.

Over the past few years there has been a growing concern over the misuse of cyber technologies for the purpose of terrorist and criminal attacks on key infrastructure. The internet now provides the world with a broad variety of opportunities to establish new methods of warfare and weaponise already existing technologies. Acknowledging the fact that the construction of cyber weapons does not require as large amounts of resources as other weapons, they can be formulated and used by a wider audience, making them weapons of extreme hazard. Even though their implications may not seem as direct as in other physically harmful weapons, they are just as lethal since they have the capability to sabotage key infrastructure and cause damage in a wide variety of sectors.

Key infrastructure, such as electricity companies or telecommunications, contains high-level targets for cyber-attacks. Any damage caused in such infrastructure disrupts normal everyday actions and disorganises a large number of people dependent on such services. The chaos created by such an attack can sometimes be the missing key for an even larger assault. For instance, if communication services went down, the military would not be able to react properly as they would not have the means necessary to organise their response, thereby allowing further criminal activity to take place. It is obvious that sabotaging major infrastructure facilities through cyber-attacks can severely disorientate a State's response to a possible attack.

In the face of this threat, it is of vital importance to understand its hazards and take measures for network security. International cooperation and trust are key components of combating cyber-attacks of all kinds and ensuring that cyberspace is a safe and lawful space used for good purposes. It is necessary to develop the capacities needed to defend ourselves against this threat and exercise the guaranteed right to self-defense while preserving the international legal order. The international community is responsible for the maintenance of peace, security and stability while ensuring that such capabilities are utilised in accordance with international law by setting global standards for the rightful use of the Internet.

Definition of Key Terms

Key infrastructure:
According to the Cambridge English Dictionary, the term infrastructure is defined as "the basic systems and services, such as transport and power supplies, that a country or organisation uses in order to work effectively".[1] Key infrastructure consists of all the physical or virtual systems and properties that fall under the jurisdiction of a State that are so indispensable that any damage caused to them could put the security, economy, public safety and health or the environment of the country in grave danger.

Cyber-attack:
The "Tallinn Manual on International Law Applicable to Cyber Warfare"[2] characterises a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". This definition applies to both international and regional armed conflict. A cyber-attack may be performed with the use of malware for the purpose of espionage, data theft, destruction of infrastructure or death of persons. However, once a cyber-attack is launched against a critical infrastructure it usually targets industrial control systems rather than stealing data.

Cyberspace:
Cyberspace refers to the worldwide online network, made up of many individual subnetworks, which connects devices internationally, facilitating communication and information-sharing. The cyberspace is closely connected to the global Internet which allows individuals to use it for entertainment, commercial, communicational or financial purposes.

Cyber weapons:
As described by the "Tallinn Manual on International Law Applicable to Cyber Warfare"[3] cyberweapons are cyber means of warfare that have the capability either by design or intent to cause damage or harm to objects or persons. Some examples of cyber weapons include viruses and malware. Cyber weapons are weapons in the form of computer code or software designed to infect individual devices or whole networks.

Cyber warfare:
Cyber warfare includes any actions taken by a state actor or international organization to damage or attack another state's networks or information systems by the use of cyber weapons, such as viruses.

Hacker:

[1] "Infrastructure." Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/infrastructure.

[2] *Tallinn Manual on International Law Applicable to Cyber Warfare*. Edited by Michael Michael N. Schmitt , Cambridge University Press, 13 May 2013, csef.ru/media/articles/3990/3990.pdf.

[3] *Tallinn Manual on International Law Applicable to Cyber Warfare*. Edited by Michael Michael N. Schmitt , Cambridge University Press, 13 May 2013, csef.ru/media/articles/3990/3990.pdf.

A hacker is characterised as a person of expertise who strives to unlawfully gain access to software or hardware.

Malware:
Malware, also known as malicious logic, is any data or instructions that may infect a device by being stored in its software, hardware or firmware which has the ability to negatively affect its performance. Some examples of malware include computer viruses or worms, trojan horses and rootkits.

Information and communication technologies (ICTs):
Information and communication technologies is a broader definition of Information Technology (IT) including all the components as well as infrastructure that enable contemporary computing. Some examples of ICTs are the internet, computers, wireless networks, software, social networks and other media that enable communication and information-sharing in a digital form.

General Overview

Cybersecurity is crucial to our welfare and safety. Malicious cyber activities jeopardise our industrial growth, liberties, and principles. Roughly half of the world's population now has access to the internet, and this percentage is continuously increasing. Even the people who are not directly linked to cyberspace are impacted by it as the agencies they depend on to supply services and products frequently use cyberspace for communicating, transportation, and finance. Improving our capability to defend ourselves against cybercrimes is critical for our future prosperity since both civilian infrastructure and military strength depend on the safe use of cyberspace. COVID-19 has marked a pivotal point in our worldwide direction, emphasizing our dependency on Information and Communication Technologies (ICTs) as never seen before. Although this catastrophe has revealed deep flaws in our society's health, education, employment and financial structures, it exposed technology's catalytic role in our coordinated response to the pandemic.

Given the borderless nature of cybercrime, interwoven cooperation in infrastructure building is vital in countering organised cybercrime and preventing breaches before they become unmanageable. Local advancement of cybersecurity policies should begin with the establishment of national building blocks. Recent cybersecurity breaches of parties such as TRITON, CPC. Corp., Moderna, and Israeli water systems demonstrated the likelihood of escalating financial damage and the number of people and countries harmed. We have already seen larger-than-ever cybercrime activities disrupting the regular growth of national economies, primarily targeting several of the state's most major elements such as industrial and financial institutions. According to the current statistics, the financial damage caused by cybercrimes is expected to exceed 6 trillion USD by 2021, equivalent to the GDP of the world's third-largest economy**.**

Both the advantages and disadvantages of cyberspace have long been debated as it may be used for both virtuous and nefarious causes. People have the opportunity of connecting to information and services without disclosing their identities because of global connection, anonymity, and loss of traceability. However, criminals have the ability of using these qualities to commit crimes. As a result, authorities, corporations, and citizens all around the planet are forced to tackle new challenges.

Authorities are concerned with protecting cyberspace, providing public services, and encouraging other significant activities but they are responsible for expanding domestic security objectives, such as law enforcement, intelligence, and military strength. Firms that are worried about securing their clients, reputations, and revenues are frequently being scrutinised, investigated, and/or asked to share data with the government. People are becoming more reliant on and appreciative of digitalization, yet they are worried about the accessibility and integrity of it. The frequency and complexity of cybersecurity threats has surged in the recent decade, particularly assaults on government networks and key infrastructures.

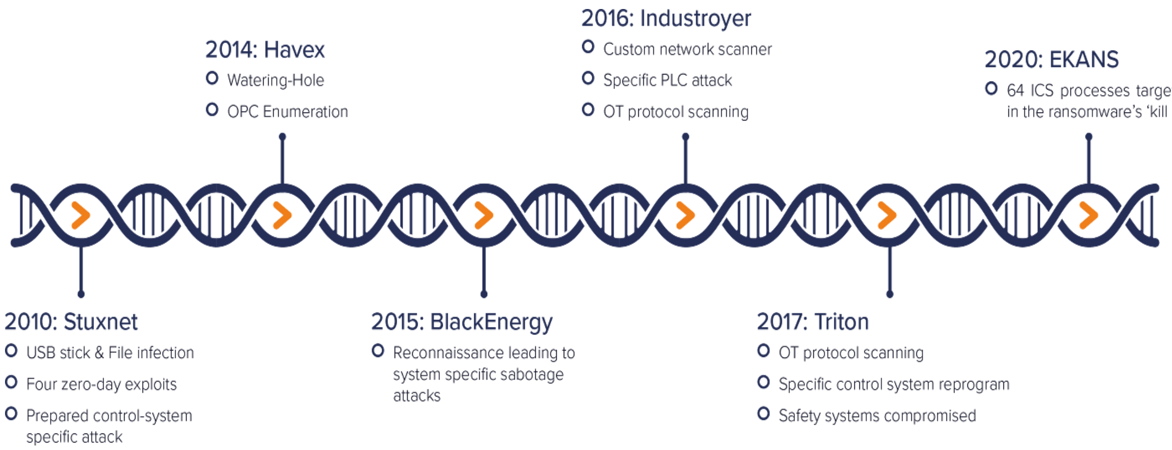
2014: Havex
Watering-Hole
OPC Enumeration
2016: Industroyer
Custom network scanner
Specific PLC attack
OT protocol scanning
2020: EKANS
64 ICS processes targeted in the ransomware's 'kill list'
2010: Stuxnet
USB stick & File infection
Four zero-day exploits
Prepared control-system specific attack
2015: BlackEnergy
Reconnaissance leading to system specific sabotage attacks
2017: Triton
OT protocol scanning
Specific control system reprogram
Safety systems compromised

Figure 1: Diagram depicting different methods used in attacks against industrial environments[4]

Although there has been many positive achievements and the increasing spread of principles, it seems that the foundation for establishing a proper normative framework on the use of ICTs, is crumbling. Various related aspects continue to compound the problem:

i. disputes amongst countries on how established principles of international law apply to governmental usage of ICTs;

ii. the reluctance of certain States in going beyond planning to rapid execution of proposed rules regarding the country's policy;

iii. an equally big incapability and resources to put the required rules and confidence-building measures in place, such as creating state institutions necessary to respond to ICT weaknesses and threats, as well as identifying ICT-related occurrences;

iv. inadequate knowledge amongst legislators;

[4] "How Cyber-Attacks Take down Critical Infrastructure." *Darktrace*, 8 July 2021, www.darktrace.com/en/blog/how-cyber-attacks-take-down-critical-infrastructure/.

v. a growing lack of confidence amongst parties, exacerbated in part by wider, non-technological factors influencing inter-state relations and hampering coordination and integration.

Multiple entities within the United Nations are engaged in pertinent ICT norm-shaping, confidence and capacity-building activities. For example, the Security Council was briefed for the first time on the use of ICTs and international peace and security. Cybercrime involving the hindering of key infrastructure was debated upon as well during the open "Arria formula" meeting.[5]

Nation-states are concentrating on key infrastructure in the energy, nuclear, water, aviation, and crucial manufacturing sectors to gather data and obtain access to industrial control systems. Such strikes include espionage, the retrieval of intellectual property, the preservation of continual network access, and laying a foundation for potential operations.

Various UN agencies and specialised bodies are assisting Member States in implementing some of these principles by raising awareness, giving advice, capacity-building, technical support, and rule-of-law-related assistance. Because of how unpredictable cyberspace is, securing and coming up with a joint strategy on tackling cybercrime and protecting key infrastructure will require considerable collaboration, cooperation, and trust-building both internationally and domestically

Major Parties Involved

United States of America (USA)

The USA, being one of the world's most powerful economies, heavily relies on the Internet and all its services are interconnected through network systems, exposing them to the threat of a cyber attack against critical infrastructure. Evidently, the country has been a victim of cyber-attacks several times in the past. In July 2021, the FBI along with the Cybersecurity and Infrastructure Security Agency (CISA) released a statement exposing Chinese State sponsored hackers that had breached the networks of thirteen pipeline operators of oil and natural gas between 2011 and 2013. Another example is the US's accusation of Russia breaching the election grid as a means to alter the results. On the other hand, the USA has also been accused of participating in cyber-attacks against other States. One prime example is the Stuxnet incident in 2010, where Iran's uranium enrichment plans seemed to be failing for no obvious reason. After investigation it was proven that they had been infected by one of the most complex viruses ever made known as Stuxnet. The US has been accused of designing said virus. However, there is no evidence to support who was behind the attack. The USA is committed to advancing their cyber security and defense mechanisms and has developed certain programs aiming to achieve such goals. Some examples include the Defense Industrial Base Cybersecurity Program by the Department of Defense, which was established as a permanent Department of Defense Program in 2013, and the Department of Homeland Security (DHS) Enhanced Cybersecurity Services (ECS) Program.

[5] "Arria-Formula Meeting On Cyber-Attacks against Critical Infrastructure." *Security Council Report*, 25 Aug. 2020, www.securitycouncilreport.org/whatsinblue/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.

Russian Federation

The Russian Federation has reached the headlines numerous times throughout the past decade, accused of having launched cyber-attacks on key infrastructure. The country has invested in hacker groups such as "Energetic Bear"[6] or "BlackEnergy" and is mostly after western oil and gas companies. The nation has breached Ukraine's electricity grid, aiming to gain access over Industrial Control Systems and disrupt their operation for their own political or financial benefit. The Russian hacker group known as Energetic Bear has also targeted major electricity companies and industrial equipment providers in Turkey, Poland, Spain, France, Italy, Germany, the US and more.

Ukraine

Ukraine has fallen victim to cyber-attacks on its key infrastructure several times in the past. Since 2014, Russia has been launching cyber operations and attacks against the state as a means to expand their geopolitical and economic goals in the region. The most notable attacks were launched in December 2015 against Ukraine's power grid. The attacks were conducted through a Trojan, known as BlackEnergy,[7] which infected Industrial Control Systems (ICS) and led to severe blackouts. The system was also hit later in 2016 by a more sophisticated attack, leaving the whole capital of Kiev dark. This malware attack is known as the "Industroyer" and was specifically designed to disrupt key industrial processes. [8]

International Police (Interpol)

Interpol is one of the main international organs committed to fighting against cyber-attacks. It facilitates investigations led by law enforcement agencies upon cybercrimes through cooperation and information sharing. Through an effective plan of capacity building, Interpol coordinates an international response to cyber-attacks by providing investigative as well as operational support, analysis, innovative research, forensics and intelligence information. Interpol provides National Cyber Reviews and has recently launched an initiative to fight cybercrime in Africa. [9]

Federal Bureau of Investigation (FBI)

The FBI is equipped with highly skilled cyber squads closely cooperating with different task forces, gathering data and the information needed to respond to the continuously evolving cyber threat. The FBI, under the Cybersecurity Information Sharing Act of 2015,[10] provides potential or already known victims with temporary clearances to access classified data so as to attempt to neutralise any ongoing threats. The Bureau also provides citizens with a hotline,

[6] CyberArk. "Meet the Energetic Bear." *CyberArk*, 18 May 2020, www.cyberark.com/resources/blog/meet-the-energetic-bear.

[7] Kaspersky. "BlackEnergy Apt Attacks in Ukraine." *Www.kaspersky.com*, 13 Jan. 2021, www.kaspersky.com/resource-center/threats/blackenergy.

[8] "Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet." *WeLiveSecurity*, 17 July 2017, www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[9] "INTERPOL Launches Initiative to Fight Cybercrime in Africa." *INTERPOL*, www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa.

[10] "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

namely the "Internet Crime Complaint Center (IC3)" which collects reports of cybercrime and cyber-attacks from the public, facilitating investigations. The FBI ensures justice to be brought to victims of malicious cyber activities with the help of legal personnel in embassies all around the globe. In addition, the CyWatch operation center is available twenty-four hours a day tracing cybercrime incidents and communicating with offices all around the world.

North Atlantic Treaty Organization (NATO)
NATO, a military alliance formed on the 4th of April 1949, is one of the strongest military alliances internationally and committed to protecting its members from a cyber-attack of any kind. The Alliance relies on strong digital defenses to protect the allies, its network, operation and data. NATO has recognised cyberspace security as a matter of priority and as of 2016 has upgraded all of its Allies cyber defense systems. All Allies are committed to information-sharing, cooperation, communication and mutual assistance so as to minimise cyber threats as well as to ensure that cyber-attacks against any of its members will be handled rapidly and properly.

Timeline of Events

2010	Stuxnet is detected in Iran's nuclear facilities
2011-2013	Chinese sponsored hackers breach 13 American pipeline operators
February 2013	The "Tallinn Manual on International Law Applicable to Cyber Warfare" is published
November 2013	The Department of Defense establishes the "Defense Industrial Base Cybersecurity Program" as a permanent program
2014-2015	BlackEnergy cyber-attacks against Ukraine's electricity grid
2015	Cybersecurity Information Sharing Act
2016	Industroyer cyber-attacks against Kiev, Ukraine.
2020	The Security Council holds the "Arria-Formula Meeting on Cyber-Attacks against Critical Infrastructure"
2021	The FBI along with the Cybersecurity and Infrastructure Security Agency (CISA) released the statement exposing the 2011-2013 Chinese cyber attacks

Possible Solutions

Increase transparency between States

In order for any measures taken to be effective and sustainable, it is essential to ensure an environment of cooperation, trust, confidentiality and transparency between all Member States. Regular reports of detected cybercrime could help States identify actors more rapidly and prevent the continuation of criminal activities. Transparency would allow the international community to achieve establishing a set of common objectives towards better cybersecurity through sharing ideas and perceptions on already implemented measures. It is necessary to promote dialogue and diplomacy between States so as to ensure that the goals set through internationally agreed upon frameworks are being respected and efforts to properly implement them are effective. Lastly, transparency between States is an indispensable piece for maintaining long-lasting stability and peace and achieving healthy multilateral relationships rooted in trust and security.

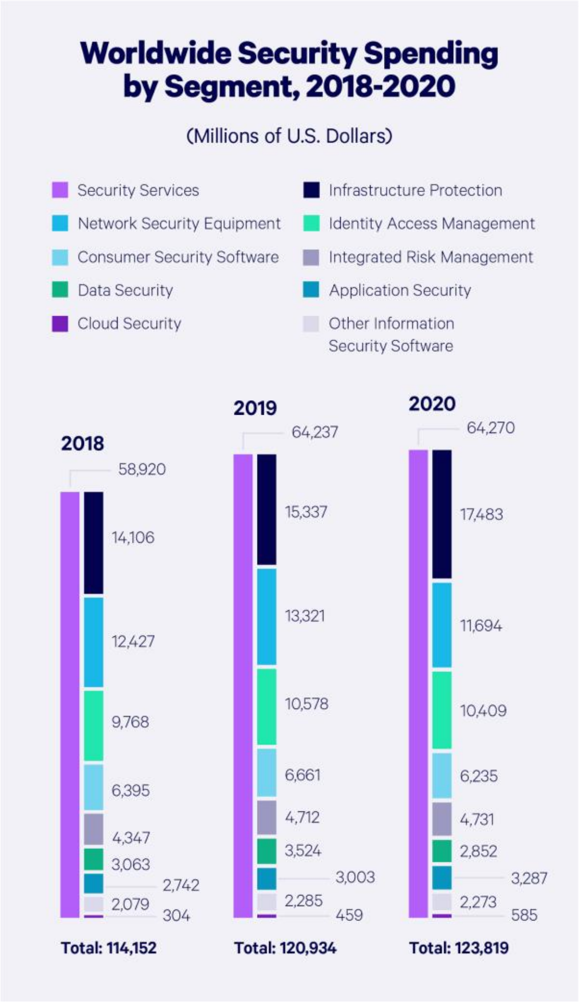

Figure 2: "2021 Must-Know Cyber Attack Statistics and Trends ." Embroker, 11 Aug. 2021, www.embroker.com/blog/cyber-attack-statistics/.

Establishment of international legal framework

Acknowledging the fact that the absence of an internationally agreed upon, legally binding framework which sets the standards for cybersecurity creates instability and insecurity, its creation and implementation is of top priority. It is of vital importance to set international standards concerning ICTs purposefully used to commit cybercrimes as a way to attack key infrastructure and ensure the protection of such facilities from cyber-attacks. A legal framework must respect a States' right to self-defense as well as their sovereignty while addressing the problem holistically. Such a framework must set clear internationally recognised definitions on cyberweapons and cyber-attacks, examine all aspects of cyber-attacks on critical infrastructure for different purposes and address issues of information-sharing between Member-States. It is also necessary that the punishment of the perpetrators as well as the framework within this should be done is also clearly stated and mandatory.

Educate technical personnel working on critical infrastructure

As the threat of cyber-attacks on key infrastructure becomes more common, it is essential to educate the working personnel of such facilities to prevent the occurrence of a possible attack. Facilities must spread awareness to their workers concerning cyber hazards through specialised training programs and ensure that they are conscious of their actions in cyberspace. It is necessary to establish ground rules concerning the usage of the Internet whilst on the facility. In addition, learning to identify certain indications of an external actor having gained access over their ICTs and/or ICS could be proven useful when aiming to minimise the effect of the attack.

Establishing an emergency response tactic

Once faced with a cyber-attack on critical infrastructure, it is of vital importance to respond rapidly and precisely. International organizations, such as the UN or Interpol, must be equipped with the technical staff necessary to cooperate with States under attack and organise a coordinated response between their different organizations and separate bodies both on a regional and international level. Acknowledging the fact that a cyber-attack on key infrastructure can influence the humanitarian, economic, political and social sector, it is essential to cooperate with different organizations simultaneously so as to address the attack holistically. Lastly, the UN provides a forum of multilateral dialogue, with the Security Council being the only body that can actively impose measures on Member States, therefore it must promote diplomacy and use its transnational influence to maintain security and stability especially during times of extreme urgency.

Bibliography

Cybersecurity | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/counterterrorism/cybersecurity.

"Infrastructure." Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/infrastructure.
Techopedia. "What Is Cyberspace? - Definition from Techopedia." *Techopedia.com*, Techopedia, 30 Sept. 2020, www.techopedia.com/definition/2493/cyberspace.

"Information and Communication Technologies (ICT)." *AIMS*, aims.fao.org/information-and-communication-technologies-ict.

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

Halpern, Sue. "How Cyber Weapons Are Changing the Landscape of Modern Warfare." *The New Yorker*, 18 July 2019, www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

Tallinn Manual on International Law Applicable to Cyber Warfare. Edited by Michael Michael N. Schmitt , Cambridge University Press, 13 May 2013, csef.ru/media/articles/3990/3990.pdf.

Clay Wilson Jun 04, 2015. "Cyber Weapons: 4 Defining Characteristics." *GCN*, gcn.com/articles/2015/06/04/cyber-weapon.aspx.

"US Says Chinese Hackers BREACHED 13 Pipeline Operators between 2011 and 2013." *The Record by Recorded Future*, 20 July 2021, therecord.media/us-says-chinese-hackers-breached-13-pipeline-operators-between-2011-and-2013/.

"Significant Cyber Incidents." *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
"US Imposes Sanctions on Russia Over Cyber-Attacks." *BBC News*, BBC, 16 Apr. 2021, www.bbc.com/news/technology-56755484.

"INTERPOL Launches Initiative to Fight Cybercrime in Africa." *INTERPOL*, www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa.

"Cybercrime." *INTERPOL*, www.interpol.int/Crimes/Cybercrime.

"Cyber Crime." *FBI*, FBI, 3 May 2016, www.fbi.gov/investigate/cyber.

"Cybersecurity Information Sharing Act of 2015 Procedures and Guidance." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

Nato. "Cyber Defence." *NATO*, 19 July 2021, www.nato.int/cps/en/natohq/topics_78170.htm.

“Arria-Formula Meeting On Cyber-Attacks against Critical Infrastructure.” *Security Council Report*, 25 Aug. 2020, www.securitycouncilreport.org/whatsinblue/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.

“Information and Communication Technologies (Ict).” *AIMS*, aims.fao.org/information-and-communication-technologies-ict.

Kaspersky. “BlackEnergy Apt Attacks in Ukraine.” *Www.kaspersky.com*, 13 Jan. 2021, www.kaspersky.com/resource-center/threats/blackenergy.

“Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity*, 17 July 2017, www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

CyberArk. “Meet the Energetic Bear.” *CyberArk*, 18 May 2020, www.cyberark.com/resources/blog/meet-the-energetic-bear.

“Analysis of Top 11 CYBER ATTACKS ON Critical Infrastructure.” FirstPoint, 28 July 2021, www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/.

“'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council IN First-Ever Debate On Cyberthreats | Meetings Coverage and Press Releases.” United Nations, United Nations, www.un.org/press/en/2021/sc14563.doc.htm.

“Secure Cyberspace and Critical Infrastructure.” Department of Homeland Security, 24 Oct. 2019, www.dhs.gov/secure-cyberspace-and-critical-infrastructure.

https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Pictures’ and Graphs’ Bibliography

Figure 1: “How Cyber-Attacks Take down Critical Infrastructure.” *Darktrace*, 8 July 2021, www.darktrace.com/en/blog/how-cyber-attacks-take-down-critical-infrastructure/.

Figure 2: “2021 Must-Know Cyber Attack Statistics and Trends .” Embroker, 11 Aug. 2021, www.embroker.com/blog/cyber-attack-statistics/.