Forum: General Assembly 1 (DISEC)

Issue: Addressing nation-state's responses towards cyberwarfare

Chair: Allyn Wang (Head Chair), Lisa Chang (Deputy Chair), Darius Hsu (Deputy Chair)

Introduction

The emergence of widespread digital technology and its advanced and advantageous utilizations in the rapidly developing world provides a convenient approach to nations' strategies in warfare. However, the detrimental effects of cyberwarfare that not only affect militants but also the cybersecurity and physical security of citizens of nations, often outweigh the benefits. Currently, threats of cybersecurity are revealed through countless reports of hacktivism and cyber espionage, where confidential and classified information is leaked and disclosed inappropriately. Taking control of missiles, unmanned vehicles is also a form of cyberwarfare that will ultimately bring catastrophe. Therefore, it is essential to tackle the issue of the rising popularity of cyberwarfare and devise effective security methods and tools.

Over the decades, nations commenced the realization of the importance and necessity of devising and responding to the threats of cyberwarfare and its effects. A variety of procedures and methods were developed to address this issue at hand such as establishing specified organizations deemed to tackle and cease the cybercrimes and attacks; another response includes shutting down Wi-Fi servers and internet services that could potentially be hacked into. Furthermore, nations' have also chosen to practice active investigations or alert the respective department of the government that controls cybersecurity.

Definition of Key Terms

Antivirus Software

Antivirus software is installed on computers to prevent, scan for, identify, and remove computer viruses. It mostly operates automatically in the background once it is installed. There are various kinds of

antivirus software that target different types of computer viruses. Programmers are constantly developing such software to keep up with the creation of new computer viruses.

Authentication Factor

Authentication factors are methods of verifying the identity of the user who is trying to gain access to a network, system, or data. There are five main types of authentication factors: knowledge factors, possession factors, inherence factors, location factors, and behavior factors. The knowledge factor asks the user to provide certain information to gain access to a system. The possession factor requires the user to have a device that is known to belong to the actual user. The inherence factor verifies the identity of the user through unique characteristics, such as handprints and fingerprints. The location factor confirms the identity of the user through his or her geographic location. Authentication factors help improve the security of the user's information and electronic devices, but there remain vulnerabilities.

Computer Worm

A computer worm is a type of self-replicating malware that spreads quickly and independently. It uses tricks to make users run it. It usually does so by disguising itself as legitimate software. Unlike computer viruses, computer worms do not need to attach themselves to existing files or programs in order to replicate, enabling them to spread easily.

Cyberattacks

A cyberattack is the action of illegally trying to harm an individual's computer, network, or other electronic devices or to gain unauthorized access to such devices with malicious intent. There are various types of cyberattacks, including spyware, worms, scareware, exploits, rootkits, and trojans.

Cybercrime

Cybercrime refers to carrying out illegal activities through the use of computers, networks, or networked devices. This includes fraud, identity theft, and privacy violations. Cybercrime is usually committed to generating profit; damaging or disabling target devices; or spreading viruses, illegal information, photographs, and other items.

Cyber Espionage

Cyber espionage, or in other words cyber spying, is a type of cyberattack in which the hacker gains unauthorized access to classified or sensitive information through technology. The goal of cyber espionage is to provide the attackers with data to gain an advantage over a competitive business or government agency.

Cybersecurity

Cybersecurity is the practice of protecting networks, electronic devices, or online information from cyber attacks. This includes defending against unauthorized access or illegal usage of such items. Cybersecurity measures involve setting strong passwords, updating software frequently, avoiding opening suspicious messages and links, backing up important files, and more.

Cyberwarfare

Cyberwarfare refers to a series of cyber attacks. It involves using computers or other technologies to attack or defend against such attacks. It may harm important systems as well as public and private infrastructures, which has the potential to cause fatalities.

Hacktivism

Hacktivism refers to the activity of using technology to break into a computer or network system. This is primarily motivated by social or political reasons rather than personal ones. It is sometimes considered activism, as one of its goals is to raise awareness of issues to initiate changes in society.

Virus

A computer virus is a type of malware that spreads between computers and causes harm to software by inserting its code into computer programs. There are various types of computer viruses, and they can be spread in different ways. One of the most common ways in which a computer can get infected by a virus is through links and attachments in emails. Computer viruses cause damage by destroying data and files, stealing sensitive information, logging keystrokes, and more.

Background Information

Historical Context of Cyberwarfare

The term “cyberwar” was first officially defined in the 2010 book, *Cyber War,* co-written by Richard Clarke, the national security advisor to Presidents Bush and Clinton and Robert Knake, who would later become the cybersecurity advisor to President Obama. The authors define this war as “actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption”. However, the meaning and knowledge of cyber war have long been acknowledged decades before. The *Omni* Magazine article in 1987, *Rise of the Mechanics,* provided a glimpse of a future where wars are fought with autonomous weapon systems, flying vehicles, and gigantic robots. The 1990s witnessed a transformation in the

conceptualization of the "imagined future", with the focus now on computers and the internet, shaping the definition of "cyber" we have today. In a 1993 RAND tank article, titled *Cyberwar is Coming*, analysts predicted a shift in military hacking from reconnaissance and espionage to disruptive attacks on enemy command-and-control systems. Their acknowledgment of the potential threat of military hackers extended beyond military computers to the destruction of critical infrastructures, creating catastrophic consequences for civilians and the nation.

The 1980s during the period of the Cold War, marked a time of great cyber advancement where the US and the Soviet Union engaged in a technological arms race to develop advanced computer technology. A decade later, the 1990s witnessed widespread internet use that pushed the risk of digital warfare and espionage to a new height. That was until the emergence of Stuxnet which officially signaled a true redefinition of cyber dangers in 2010. Holding an unprecedented and undiscovered level of complexity, the Stuxnet was a computer worm designed by the U.S. and Israeli intelligence as a means of disabling a key part of the Iranian nuclear program. Constituting as one of if not the most complex cyberwarfare attacks the world has seen, the level of sophistication of the piece of code was undeniably an attack that changed the world's perception of cyberwar. It has been recognized to be the first cyberattack ever designed to directly damage physical equipment (the centrifuges in Iran's nuclear enrichment facilities). The incident acted as a catalyst that fueled the ignition of the global cyber arms race in the following years.

Cyberthreats in the Present Day

Cybersecurity on a Global Scale

With the increase of information and communication technologies (ICT) utilized around the globe, the vulnerability of citizens, private entities, and governments to malicious cyber activities goes on the rise. Specifically, the threat of cyberwarfare has become more prevalent than ever in the modern day. Amidst geopolitical and economic tensions, state-sponsored cyberwarfare has emerged as a pressing concern for nations globally, with the US labeling cyber threats as the top threat to US national security, surpassing physical weapons and terrorism.

The lack of universal consensus on the definition of cyberattacks and cyberwarfare and what constitutes as these incidents should not prohibit states in the modern day from establishing immediate protocols and safety nets to combat potential cyber threats. With more than 100 governments developing national cyber security defense strategies to combat these risks, it becomes more evident than ever the concern over cyber warfare. However, even with the number of regulations and procedures being instituted on a global scale, the threat of cyberwar does not shrink, especially in the present day. Spanning from espionage missions to the

spreading of propaganda, cyberwarfare attacks are not limited to the penetration of military attacks. In the context of existing conflict and tension between nations, the consequences of cyber threats become even more prevalent. Amid Russia's invasion of Ukraine's eastern region and Crimean Penisula, the first-ever blackout induced by a cyber attack occurred leaving hundreds of thousands of Ukrainians without power in their homes. The attack was followed by a series of data-destroying attacks targetting Ukraine's capital. The following year, with the release of NotPetya malware, Russia's cyberwar against Ukraine reached its climax with the destruction of banks, and ATMs and the paralyzation of critical infrastructures including government agencies and hospitals.

Through this incident, it is important to analyze the increasing danger of cyber attack consequences in the context of physical tensions between nations, moreover, the path that should be taken towards better cybersecurity on a global scale. It seems simple for governments and private sectors to take first steps on a financial aspect, by investing more in hardening their networks and separating crucial systems from the internet to decrease exposure to the public. However, in the presence of cyberwars of the 21st century, no amount or level of cyber security technology can be enough to shield all future attacks. What critical infrastructure operators and government agencies must prioritize is the building of robust systems of cyber resilience that enable them to swiftly recover from these severe cyber attacks.

Accountability in Cyberwarfare amidst International Norms and Repercussions

The issue of accountability takes center stage as nations grapple with the consequences of launching cyber attacks that breach internationally established red lines. In the landscape of cyber threats on a geopolitical scale, nation-states should become well aware of these customary guidelines that define acceptable and unacceptable cyber activities as well as the emphasis on the global norms on this matter. The call for serious repercussions on those who violate these matters should be echoed throughout international discussions across global bodies. However, this becomes increasingly intricate with cyber policy challenges and the fear of escalation in response to cyberattacks or threats.

Advocating for a global treaty or convention becomes much more complicated at this time as the call for explicit rules in cyberwarfare remains largely unheeded. Notably, both NATO and the UN lack explicit regulations on this matter, with the Tallinn Manual by NATO CCD COE serving as the only non-binding international manual that studies how international law can be applied to cyber warfare. Cyberpeace initiatives have gained traction, yet critics continue to highlight the obstacle in defining cyberattack motives in addition to the complexity of determining the identities of the hackers responsible. A more fundamental barrier lies in the nation's government's reluctance to commit to cyberwar limitation agreements, especially the

super-powers of the decade. Their fear of imposing restrictions on their nation's freedom to launch cyber attacks against others becomes a central factor in the inability to establish cyber security and trust on a global scale.

Adding to these complexities, there exists a pervasive fear of escalating tensions when countries experience cyber threats or attacks. This fear stems from the fact of realization that attributing cyber incidents to specific parties can create hostility that may end up jeopardizing the nation's safety. There is thus a prevailing hesitation to respond forcefully even when there may be sufficient evidence to pinpoint the origin of such attacks. The responses below provide a glimpse of notable incidents in history in which governments have chosen to take specific steps or procedures in response to cyber-attacks, many of which may be similar or largely different depending on the nation's decision of action during that time.

Nation responses towards notable cyber incidents in history

Estonia 2007: An alleged Distributed Denial of Service (DDoS) cyberattack by the Russian Federation targetting large Estonia's cyberinfrastructures. By shutting down the websites of ministries, banks, media, and political parties, the incident did not result in large-scale nationwide damage but some minor economic damage. The government's response to this was done through their Computer Emergency Response Team (CERT) connected to the Estonian Ministry of Economic Affairs and Communications. The CERT's immediate procedures included closing down websites under attack for foreign internet traffic and collaborating with cybersecurity experts from various European countries to share intel intelligence on the situation. Other than such nations, organizations including the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) and the EU also facilitated political network channels to increase cyber attention on a long-term scale.

Saudi Arabia 2012: In August of 2012, the nation experienced a cyberattack directed at its biggest company, the state oil company Saudi Aramco. The attack may have caused substantial damage to the Saudi economy and perhaps impacted the global economic flow if it had been successful with its goal to disrupt oil and gas production in Saudia Arabia. Through examining open sources, it appears that the primary entity responding to the attack was not the Saudi Ministry of Foreign Affairs, but rather the company that established its countermeasures towards the incident. The Ministry of Interior also played a role in response to the incident by assisting Saudi Aramco with active investigations on the origin and damaging effects of the attack.

South Korea 2013: The nation frequently faces cyber attacks, most notably from the Democratic People's Republic of Korea (DPRK). It has been noted by certain sources that this has reached a day-to-day frequency. The appearance of the malware "Dark Seoul", marked the largest cyber-attack carried out against South Korea, targeting major banks and national television broadcasting stations.

While the incident was widely attributed to the DPRK, no explicit claim of responsibility for the attack was made. On the governmental level, various ministries and governmental organizations were active in responding to the incident alongside the banks and stations that were focused primarily on restoring their systems. The Ministry of Defence and the military heightened their alert status against potential cyber-attacks and chose not to establish accusations against anyone. In hindsight, there was no mention of any foreign policy activities on the cyberattack, indicating the likelihood that the South Korean government domestically resolved the situation to prevent further escalations with the DPRK.

United States 2014 (Sony Pictures Incident): Perhaps one of the most notable cyber incidents in the 21st century, Sony Pictures Entertainment became the target of a cyberattack in 2014 as hackers under the name name “Guardians of Peace” released confidential data from the company as well as implementing software programs to erase data from servers. Initially, the hackers demanded financial compensation to stop their attack, but later changed their demands to the cancellation of the upcoming release of “The Interview”, a comedy revolving around the assassination of Kim Jong Un. Not only did the media quickly link the attack and threats to the DPRK, but the US government declared the incident as a matter concerning national security with statements addressed by President Obama and the Secretary of Homeland Security. Initially refraining from attributing the attack to any specific country in an effort to not raise intergovernmental escalations, the US government, however, was reported to have initiated actions after the FBI formally announced sufficient evidence linking the government of DPRK to the attack. By requesting small-scale economic sanctions to be placed on the DPRK and the execution of statements from the white house, the US expresses their intolerance of cyberattacks directed at their companies and their impact on their citizens and state.

The impacts of cyberwarfare

Economic Ramifications:

Cyber attacks have the potential to inflict severe economic repercussions not only on individual businesses but also on a nationwide scale. It is estimated that global cybercrime has amounted to costing the world’s economy a near 600 billion, with 0.8% of GDP lost annually. The disruption of financial systems by these attacks poses as a significant concern that directly impacts the economy and individuals. These systems are the backbone of economic operations constituting banks, stock exchanges, and other key components which facilitate the flow of capital. When targeted, the risk of operational disruptions surges rapidly giving way to the appearance of market volatility, financial losses affecting individuals and private entities, and the reignition of increased identity thefts. Amidst these impending concerns, the potential jeopardization of the National Economic Stability peaks as a core concern. A significant cyberattack may possess the capability to destabilize an entire nation’s economy

by triggering systemic repercussions. Furthermore, the potential impact on the nation's GDP is a critical matter that cannot be overlooked in the present day.

Critical Infrastructure Vulnerabilities:

Power grids, water supplies, communication networks, and hospitals all constitute as critical infrastructures in every state around the world. The potential prospect that these infrastructures could be destroyed physically on a virtual scale in a matter of seconds becomes a factor of great concern. The matter becomes even more critical when addressing public safety and ensuring the continued provision of essential services to the public.

Political Landscape Disturbances:

When discussing the issue at hand, with nation-state responses to cyber threats and attacks, we have to look into the impacts in a geopolitical context. With the year-over-year growth of these incidents, governments around the world have largely been able to comprehend the short and long-term disturbances of cyber incidents. On a short-term scale, the impact of these attacks has shown to be serious and immediate when initiated. In 2014, the U.S. government was subjected to more than 60 thousand cyber security breaches, with a single one of those breaches resulting in the loss of 14 million records of confidential information that included social security numbers of current and former government officials. Accessing geopolitical shifts and considering diplomatic repercussions becomes essential when examining the long-term impacts of these attacks Tensions across diplomatic ties, changes in nation-to-nation relationships, and the challenge of building future alliances and trust all correlate to the effects of that cyberattacks can bring to the geopolitical landscape of the 21st century.

Caption #1: The United Nations Logo

Major Countries and Organizations Involved

Russian Federation

Russia has emerged as a significant player amongst other notable cyber nations of the 21st century. The nation's engagement in cyberspace and its role in instituting offensive cyber operations in its conflict with Ukraine has become a notable concern in the international community. As of 2022, there is no unified regulation on cybersecurity in Russia amidst the many "general principles" that may be applied to particular cases and activities.

United States of America

The U.S. a pronounced member of the top most powerful cybernations in the world has made significant progress towards the advancement of cybersecurity and the planning of cyberstrategies. Achieving a perfect score of 100 on the Global Cybersecurity Index in 2022 is evidence of the nation's dedication to these goals. Their 2023 DOD Cyber Strategy informs of the insights gained through the years of executing cyber operations and encountering cyber threats, as well as the close observation of the utilization of cyber tactics in the context of the Russo-Ukraine war.

China

The PRC, a key actor in the realm of cyberwars, serves as an economic superpower of the present day. In recent years, the nation's cyber pursuits and alleged cyber and industrial espionage incidents have garnered the concern of many, especially the U.S. The Chinese Communist Party (CCP) has been noted to "demonstrate the willingness to use its capabilities to project power". Tensions in the Taiwan Strait also become a key area in which nations believe China would engage in cyber attacks that could potentially damage critical infrastructure networks. The concern extends to the belief that the CCP's attacks may underscore China's objective of gaining economic and military advantages through the exfiltration of sensitive information from military and political targets.

North Korea

The DPRK has notably gained a reputation as one of the world's most advanced and sophisticated cyber nations, as the Office of the Director of National Intelligence (ODNI) states that the nation's cyber program "poses as a sophisticated and agile espionage, cybercrime and attack threat…". With a large and well-funded military and similar-sized *civilian cyber workforce,* North Korea's cyber activities have largely been recognized as serious and consequential. Its recent ransome campaigns against Health and Public Health Sector organizations in addiiton to other critical infrastructures, showcase the nation's significant evolvement in the cyber domain. In a study done by the Korean Economic Institute, the DPRK has plans to enhance its cyber-attacks and defense with AI by putting forth a significant amount of resources towards the research of the latest technologies and the creation of large-scale cyber units within its military.

Iran

Iran in the last decade has grown to stand as a major cybernation, with the ODNI expressing the nation's remains as a substantial cyber threat. Following the 2010 incident with Stuxnet, the nation of Iran joins the arms race, now as the aggressor and not the victim. Its recent activities have constituted destructive malware and ransomware operations. The nation's growing expertise and willingness to conduct serious cyber operations is what triggers the worries of the international community that sees it as a threat to international security. By housing a large and sophisticated cyber workforce, Iran has been subjected to numerous allegations of malicious cyber activities as well as demands for accountability for these actions.

Israel

Israel, a victim natio to hundreds and thousands of cyber-attacks monthly, ranging from states to hacker groups, to individuals, lies at the center of a cyber security industry worth $82 billion. This has thus forced the nation to be heavily reliant on cybertechnology in addition to constantly developing and improving advanced cyber capabilities. As a notable cyber power operating in the present day, Israel may be viewed as a model for other states in terms of navigating and utilizing cyberspace, both "offensively and defensively". A key factor that makes this nation a leader in the cyber domain, is its government's willingness and activeness in facilitating cybersecurity expertise through investments into its human capital, collaborations with National Task Forces, and leveraging its nation's military. In this way, Israel can remain a "cyber superpower" even with the emergence of other influential powers in the modern world.

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

A NATO-accredited research and training facility was established to deal with aspects of cybersecurity including education, research, and development. As of today, 22 nations and 3 contributing participants are sponsors of this hub of cyber defense expertise with the untied mission to enhance the capability, cooperation, and information sharing amongst NATO nations on cyber defense. The Tallin Manual published by NATO CCD COE has been an important instrument as of the present day dictating the applicability of international law on cyberwarfare.

European Union (EU)

A political and economic union consisting of 27 member states, the EU was established during the aftermath of WWII with the goal of promoting peace, stability, and prosperity in Europe. In the present day, this has spanned various fronts including that of the cyber-scale, by promoting cyber resilience and the defense of data and communication, helping to secure the online society and the economy.

Cybercrime was labeled as a top priority for the EU within the *EPACT 2022-2025* to fight against serious and organized crimes. Since this form of crime and threat is prevalent in EU member states, it becomes increasingly crucial for the union to foster cyber diplomacy and defense for the international community.

African Union (AU)

A continental union consisting of 55 member states located on the African continent, its mission is to promote the unity and solidarity of African countries, including that within cyberspace. The Draft African Union Convention on the Establishment of Credible Framework for Cybersecurity in Africa, drafted by the union in 2011, establishes a credible framework for cybersecurity in the countries. The convention criminalizes a wide range of cyberactivity including hacking, identity theft, and cyberfraud in addition to entailing procedures for the investigations and prosecutions of cyber crimes.

Timeline of Events

Date	Description of event
November 2, 1988	The Morris Worm, a computer worm, was released. It was created by Robert Tappan Morris.
September 1999	A teenage boy, Jonathan James, hacked into the computers of the U.S. Department of Defense (DOD). With his access to the DOD's computer system, he stole the software that NASA used to maintain the International Space Station.
August 2008	Russian forces launched cyberattacks on the Georgian government and network infrastructures, which disabled the country's web-based communication with the outside world. Then, the Russians invaded Georgia.
2009	President Barack Obama announced the establishment of a Cybersecurity Coordinator position within the National Security Council and the National Economic Council. This individual was in charge of implementing cybersecurity policies and strategies.
January 12, 2010	Hackers engaged in cyber espionage and invaded Google's servers. They gained access to the Gmail accounts of human rights activists in China. This was followed by an investigation through which authorities found out that this had happened to many people around the world.

November 2010	England reveals its plan to allocate 1 billion dollars for the development of new cyber defenses.
December 2010	The Interior Ministry of Germany announces its plans to establish a national cyber defense center.
December 2010	The Cyber Conflict Studies Association reveals that over 100 countries had the ability to engage in cyber conflicts.
January 2011	Estonia revealed its intentions to establish the Cyber Defense League, where a group of volunteer scientists and individuals would form a militia and function under military command.
September 2011	In Nevada, malware infected the networks at Creech Air Force Base. There were no significant damages; however, the malware was challenging to remove.
December 2019	The General Assembly of the United Nations voted to start negotiations for a treaty to address cybercrime.

Relevant UN Resolutions and Treaties

- Combating the criminal misuse of information technologies, 22 January 2001 **(A/RES/55/63)**
- Combating the criminal misuse of information technologies, 23 January 2002 **(A/RES/56/121)**
- Creation of a global culture of cybersecurity, 31 January 2003 **(A/RES/57/239)**
- Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004 **(A/RES/58/199)**
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, March 2010 **(A/RES/64/211)**
- Countering the use of information and communications technologies for criminal purposes, 20 January 2020 **(A/RES/74/274)**
- Countering the use of information and communications technologies for criminal purposes, 1 June 2021 **(A/RES/75/282)**

Possible Solutions

Active Investment or Advancements in Cybersecurity Infrastructures

Countless successful cyberattacks result from the weakness and vulnerability of the current cybersecurity infrastructures of nations. Therefore a plausible solution is to increase the security of cybersecurity infrastructures. By collaborating with industry professionals and leaders and implementing effective authentication methods such as firewalls, which can constructively prevent and decrease the number of cyberattacks. Additionally, the strengthening of cybersecurity infrastructures can also ensure and protect network boundaries. While this method may be effective in defending nations against hijackers and cyber attackers, it does not prevent or cease the attacks of the cyber offenders. Furthermore, ways to overpass the strengthened security systems will eventually be devised in the world of rapidly developing technology.

Increasing international cooperation and encouraging the exchange of information regarding cyberwarfare to address regional challenges

In order to keep track of records of cyberattacks and documenting data, it is important to increase international cooperation and encourage the exchange of information. Engaging and collaborating with other fellow nations to share developed intelligence and practices can be an effective way for LEDCs to also synchronize their technology development with MEDCs against the threat of cyberwarfare. This can also create and establish international agreements and regulations between nations.

Unification of public awareness campaigns

People with a lack of knowledge or insufficient awareness in the field of cybersecurity have a high chance of placing themselves in jeopardy. It is essential to provide unified education campaigns and input said subjects in curriculums or education programs and schools. Furthermore, adults and the elderly who has had limited interaction experience with cybersecurity should also be informed about the issue with cyberwarfare. Speeches by professionals , posters, or social media are all platforms that could potentially be used to spread awareness and education. It is necessary to acknowledge that the spread of fake information could be possible, therefore hiring professionals or organizations to verify the information on these platforms is crucial.

Questions for Further Research

1. What factors contribute to certain nations' success in terms of cyberwarfare regulation?
2. What roles do cultural factors play in the vulnerability of cybersecurity?
3. What are the reasons for the varying perspectives of nations in establishing goals regarding cyberwarfare?
4. How does the current implementations of infrastructures' failure to address the issue in certain nations reflect their vulnerability?

5. What are the long-term and short-term effects of establishing regulations and policies of nations?

Bibliography

"African Union (AU)." The Nuclear Threat Initiative, James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, 30 June 2019, www.nti.org/education-center/treaties-and-regimes/african-union-au/#:~:text=The%20African%20Union%20was%20established,and%20harmonize%20Member%20States'%20policies.

Atrews, RA. "Cyberwarfare: Threats, Security, Attacks, and Impact." Journal of Information Warfare, vol. 19, no. 4, 2020, pp. 17–28. JSTOR, https://www.jstor.org/stable/27033642.

"A UN Treaty on Cybercrime En Route." *United Nations Western Europe*, United Nations, 23 June 2022, unric.org/en/a-un-treaty-on-cybercrime-en-route/.

Cohen, Matthew S., et al. "Israel and Cyberspace: Unique Threat and Response." International Studies Perspectives, vol. 17, no. 3, 2016, pp. 307–21. JSTOR, https://www.jstor.org/stable/26393471.

Greenberg, Andy. "Cyberwar: The Complete Guide." Wired, Conde Nast, 23 Aug. 2019, www.wired.com/story/cyberwar-guide/.

"Iran Cyber Threat Overview and Advisories: CISA." Cisa.Gov, Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran.

Meer, Sico van der. Foreign Policy Responses to International Cyber-Attacks Some Lessons Learned, Clingendael: Netherlands Institute of International Relations, www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf.

Montgomery, Mark, and Jiwon Ma. "Defense Department Report Highlights Cyber Threat from China." FDD, Foundation for Defense of Democracies, 6 Nov. 2023, www.fdd.org/analysis/2023/11/06/defense-department-report-highlights-cyber-threat-from-china/.

"North Korea Cyber Threat Overview and Advisories." Cisa.Gov, Cybersecurity & Infrastructure Security Agency, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.

Parsons, Andrew. “Rise of Cyber Warfare: The Growing Threat of Cyber-Attacks in Modern Conflicts and the Impact on Businesses (Guest Blog by Womble Bond Dickinson).” The UK’s Technology Trade Association, techuk.org, 20 Jan. 2023, www.techuk.org/resource/natsec2023-wbd-20jan23.html.

Talihärm, Anna Maria. “Towards Cyberpeace: Managing Cyberwar through International Cooperation.” United Nations, United Nations, Aug. 2013, www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

“The 10 Most Powerful Cyber Nations in the World.” Humanize, 13 Feb. 2023, www.humanize.security/blog/cyber-awareness/the-10-most-powerful-cyber-nations-in-the-world.

“What Is Cybersecurity?: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, Cybersecurity and Infrastructure Security Agency CISA, 24 Jan. 2024, www.cisa.gov/news-events/news/what-cybersecurity.

“What Is a Cyber War – Explained.” NEIT, New England Institute of Technology , 30 Mar. 2023, https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=The%20history%20of%20cyber%20warfare%20goes%20back%20to%20the%201980s,digital%20warfare%20and%20espionage%20increased.

“UN Resolutions.” *ITU*, ITU, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

Vadakkanmarveettil, Jyotsna. “Why the Israelis Lead the World in Cyber Security Expertise?” UNext, 27 Jan. 2020, u-next.com/blogs/cyber-security/why-the-israelis-lead-the-world-in-cyber-security-expertise/#:~:text=In%20modern%20day%20Israel%2C%20there,centers%20dedicated%20to%20cyber%20security.&text=The%20Israeli%20government%20along%20with,a%20superpower%20in%20cyber%20security.