PacificMUN

Dare to Speak

DISEC-Topic B
Backgrounder Guide

Letter from the Director

Dear Delegates,

My name is Emily Ni, and it is my utmost pleasure to welcome you to the Disarmament and International Security Committee (DISEC) at PacificMUN 2019.

Ever since my first experience three years ago in a General Assembly, I've been enamored with the passionate discourse found uniquely within Model UN. I can say with absolute conviction that the people you meet, the topics in which you gain immense amounts of knowledge, and the skills that you develop as a collaborator, public speaker, and delegate, are invaluable to you. I can only hope to instill the same passion in you, the delegate, as my directors did for me.

Serving as your two Chairs are Steven Long and Rhéa Tabet. Steven is currently a grade 11 student at St. George's school, and is looking forward to making PacificMUN a memorable experience for all. Rhéa is ecstatic to be serving as your Chair at PacificMUN 2019, and is currently a grade 11 student at École Secondaire Jules Verne.

Maintaining international peace and security are DISEC's ultimate goals. Therefore, delegates must work to draft comprehensive resolutions that maintain global stability. Both our topics are incredibly expansive and require thorough research to allow for constructive debate. Therefore, I would like to stress the importance of gaining an extensive understanding of your country's stance and relationship with the topics at hand in order to allow for an engaging experience; your work as a delegate will not only benefit yourself, but the committee as a whole.

The entire dais team welcomes you to the Disarmament and International Security Committee at PacificMUN 2019. Please do not hesitate to contact us if you have any questions or concerns; we look forward to a weekend of rewarding debate.

Sincerely,

Emily Ni
Director of DISEC
PacificMUN 2019

Committee Overview

On January 24th 1946, the first resolution of the First Committee, the *Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy*[1], was adopted by the United Nations.

Created in 1945 following the atrocities witnessed in World War II, the Disarmament and International Security Committee (DISEC) plays an integral role in maintaining international security and stability. In the First Committee of the United Nations, all 193 members of DISEC play an integral role in maintaining world peace.

Ever since its inception, a newly created First Committee resolved to succeed where the League of Nations had previously failed. Replacing the defunct intergovernmental organization created to maintain stability after World War I, the UN and DISEC specifically have grown to encompass a plethora of pressing international issues ranging from asymmetric warfare to cybersecurity. Although unable to make binding resolutions, DISEC is able to recommend effective solutions that broaden the limited scope of the UNSC. Unique to DISEC is its entitlement to verbatim records coverage, the only Main Committee of the General Assembly able to do so. Its size and scope make it an invaluable organ of the United Nations, offering multifaceted opinions on far-reaching international issues. The considerations and recommendations that DISEC, as part of the General Assembly, is able to offer, are crucial to the United Nations (UN).

The most pertinent global conflicts are subject to heated debate and tentative resolution in DISEC. Most recently, the 72nd session resulted in a multitude of resolutions on topics almost as extensive as the scope of the committee itself. From peacekeeping operations in every corner of the globe to the risk of nuclear proliferation in the Middle East, DISEC's ultimate responsibility is to ensure international security. The committee also works extensively with the United Nations Disarmament Commission (UNODA), as

[1] http://www.un.org/documents/ga/res/1/ares1.htm

well as numerous non-governmental organizations (NGOs) that allow for insightful contribution to its resolutions. DISEC's work in the international community is with marked with significant funding. The estimated budget for 2016-2017 was nearly 5.4 billion[2], and it is clear that the funds allocated to this committee have made notable changes for the better.

Topic B: Cyber Warfare in the 21st Century

Introduction

With rapid technological advancements on the rise in the 21st century, cyber warfare has become a pressing concern for the entire international community. Along with the many tangible benefits, brought by the rise of the Internet, it has also brought with it an onslaught of cyber attacks that jeopardize the security of billions across the globe. With cyber attacks on the rise, hackers have the ability to shut off power grids and other critical infrastructure at will. From Russian meddling in American elections[3] to the destruction of Iranian nuclear facilities[4], these attacks have proved to be devastating in their effect. With global tensions rising and world leaders seemingly at odds with each other, the risk of a full-scale international cyberwar is constantly rising.

These cyber attacks are devastating, and their repercussions can be felt in every corner of the globe. There exist two distinct categories of cyberattacks: guerrilla and state-supported. There is still room for definitional debate on the terms' ambiguity, but it is widely accepted that the distinction is simply whether or not the attack is supported by a nation. Moreover, the ramifications of a state-supported attack are much more detrimental on a political level, straining international relations. Oftentimes, a state will sponsor an attack on an enemy state to further their political agenda. A notable example of a large state-supported attack is the Stuxnet worm. A joint Israeli-American project, it was discovered that approximately a fifth of Iran's nuclear centrifuges were destroyed by the virus.[5] Guerrilla attacks, on the other hand, are no less destructive. The large Equifax data breach of 2017 compromised the private information of roughly 149.7 million people in the US alone.[6] Finding ways to defend against these attacks is extremely important in protecting international security.

The most dangerous situation is the potential for a large-scale attack on critical infrastructure. Energy grids, hospitals, even pipelines: these are all at risk of being crippled beyond use. There must be measures put in place to defend against these large scale attacks that could potentially devastate a

[2] http://www.un.org/en/ga/fifth/70/ppb1617sg.shtml
[3] https://www.bbc.com/news/world-us-canada-44825345
[4] http://large.stanford.edu/courses/2015/ph241/holloway1/
[5] http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
[6] https://www.thestar.com/business/economy/2018/03/01/equifax-finds-additional-24-million-in-us-impacted-by-2017-data-breach.html

large demographic of any given country. When a cyberattack directly damages infrastructure providing water, electricity, defense systems, communications, and health services, citizens and governments alike will undoubtedly suffer at the hands of cyberwarfare.

Timeline

1969 - The Advanced Research Projects Agency (later known as DARPA) develops a network intended to link computers at research institutions funded by the Pentagon. This initial project was called ARPANET and eventually evolved into the modern Internet.

November 2nd, 1988 - A graduate student at Cornell University, Robert Morris, released the first computer "worm". A flaw in his design led to the widespread infection of computers and brought much attention to Internet security. Morris was consequently the first person tried and punished under Congress' new *Computer Fraud and Abuse Act* of 1986.

November 2003 - Chinese hackers, assumed to be part of the People's Liberation Army, launched a barrage of coordinated attacks on US government computer systems. Dubbed "Titan Rain" by US investigators, they infiltrated and compromised a number of government agencies, notably the US Department of Defense.

April 27th, 2007 - A decision to move a Soviet memorial to the outskirts of Tallinn, Estonia, prompted outrage in Russia. Botnets took down banks, government services, and media outlets all over Estonia. The attacks were attributed to Russian hackers, but it is still unclear if the attack was state-supported.

July-August 2008 - Major cyber attacks on Georgia occurred in tandem with the Russo-Georgian war. By August, the President's website was defaced with images of Adolf Hitler, the Parliament's website had been similarly attacked, and the National Bank of Georgia was also hit.

January 2009 - During Israel's military offensive in the Gaza strip, at least 5,000,000 Hamas computers attacked Israeli internet infrastructure and government websites. The operation was funded by either Hamas or Hezbollah and reportedly carried out by a criminal organization in the former USSR.

2010 - Stuxnet, a highly sophisticated piece of malware, succeeded in its goal to derail Iran's nuclear program. The worm was responsible for the destruction of one fifth of Iran's nuclear centrifuges and was created as a joint US-Israeli project (although neither country has openly admitted responsibility for the attacks).

November 2011 - Over the course of 2011, at least 10 major Norwegian defense and energy companies were hacked: passwords, confidential documents, and data all were compromised. Norway's National Security Agency (NSM) reported that the attacks occurred when the companies were involved in major contract negotiation.

June 25th, 2012 - The director-general of MI5 and head of UK Security Service stated that a major London-based company had lost "*some £800m" ($1.2 billion) to state-sponsored cyber-attack*[7].

November 2014 - North Korean hackers attack Sony Pictures Entertainment in retaliation against the controversial film, "The Interview." They posted employees' personal information and leaked confidential data.

April 2015 - French public TV network TV5Monde was attacked by hackers who claimed to be affiliated with ISIS. The network's website and social media accounts were defaced with pro-ISIS imagery. Additionally, 11 of the network's channels were taken off the air.

February 2016 - Banks in Ecuador, Vietnam, and the Philippines were all hacked by the DPRK. They are also suspected of hacking into the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network in order to steal $101 million from the Bangladeshi Central Bank.

December 2016 - In Northern Kiev, a cyber attack on Ukraine's national power company caused a power outage for over an hour. Hackers had been able to hide undetected in Ukrenergo's network for six months prior to the attack. Ukrainian security services blamed the attack, similar to one attributable to the Kremlin in 2015, to Russia.

September 2017 - Equifax was affected by a hack that compromised 143 million users' personal information including 209,000 credit card numbers. The data breach took place in July, but the credit monitoring firm only disclosed months later.

Historical Analysis

From the humble beginnings of the Morris worm, the size and scope of cyber attacks have grown exponentially. In the early 2000s, when cyberwarfare was still a relatively new concept, major attacks were extremely alarming to global superpowers. The ability for another nation to gain access to highly sensitive information with ease was shocking and a large threat to national security. The attacks that took place at this time were met with little resistance, mostly due to the fact that they were extremely

[7] https://www.economist.com/business/2012/06/30/a-spook-speaks

underprepared to defend against this new type of warfare. However, the impacts that these attacks had were mitigated by the fact that cyber warfare was so new. The initial major actors with a large stake in these newfound attacks were China, the US, and
post-Soviet states. They also revealed the threat that cyberwarfare posed to nation-states. With technological advancements on the rise, look back to several notable attacks that shaped the evolution of cyber warfare itself. It becomes evident through further analysis that as the technology used for these hacks changes, so does the nature of what they intend to achieve. Evolving from information gathering, or infiltration of government databases, the nature of cyberattacks has changed over time to exploit the poorly guarded flaws in government services themselves. These changes resulting from shifts in government and individual incentives have manifested themselves in larger attacks that target essential services or larger targets like corporations. With the evolution of cyberwarfare, and with rapid technological advancements constantly furthering development, the scale and scope of cyberattacks have grown exponentially.

2007 Estonian Attacks

Spurred as a response to a controversial decision to move the Bronze Soldier - a Soviet symbol of historic Estonian oppression - to the outskirts of the country, numerous crippling attacks were launched on corporate and government sites, leaving banks, newspapers, media outlets, government sites, and emails all unable to function throughout April and May of 2007. For “one of Europe’s most wired countries,”[8] the attack was incredibly disruptive and shed light on the power a cyberattack can hold over countries as a whole.

In particular, these hacks highlighted the difficulties that governments face in retaliation and defense, due to the shadowy nature of cyber warfare. Unlike traditional warfare, it becomes extremely difficult to pinpoint the sources behind these crippling attacks. Purposefully concealing the source of cyberattacks is common practice, and it is often a long and arduous process to uncover the source of a carefully concealed attack. Even for a NATO country like Estonia, the gate is open for a state-sponsored attack without fear of retaliation from its allies. Additionally, because of the confusion caused, it is onerous to pinpoint the source of the attack and retaliate accordingly. This becomes evident upon analysis of the Estonian cyber attacks: it is still unclear as to who truly orchestrated the attacks.

Although there is no conclusive evidence to this day, the Estonian government still blames the Kremlin for the destructive attacks. This leaves the door open for future development; delegates should keep in mind the importance of tracing attacks, as well as the importance of identifying guerilla and state-supported attacks in order to deal with them accordingly.

[8] http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.W2N1sNhKjpA

Stuxnet Worm

Beginning under the Bush administration and continued under Obama, the joint Israeli-American virus known as *Operation Olympic Games* was a nonviolent alternative to slow Iranian nuclear development.[9] Destroying approximately 1,000 of Iran's 6,000 centrifuges, the Stuxnet worm serves as a prime example of a devastatingly effective state-sponsored attack.[10] The orchestration of a fully state-sponsored attack on a foreign sector like nuclear energy opened the door for overt cyberwarfare as a legitimate means through which governments could directly attack critical sectors. It reshaped the landscape of cyberattacks completely - no longer were attacks on power plants science fiction: the Stuxnet worm cemented infrastructural attacks into legitimate means of cyberwarfare. Note the importance of major actors like Israel and the US using weapons that clearly violate international law to further their own agendas and intervene in the Middle East, especially considering the current and historical geopolitical tensions that exist within the region. The Stuxnet Worm is one of the most notable examples of a state-sponsored attack that exacerbated asymmetric cyberwarfare, and proves the importance of cyberattacks in international politics.

Current Situation

2016 Election Meddling

Russian hackers interfering with the 2016 US presidential election employed phishing emails and malware to damage Hillary Clinton's campaign, all the while supporting Donald Trump and other candidates.[11] In March of 2016, the chairman of Clinton's campaign, John Podesta, unknowingly shared his password with hackers as a result of a simple phishing email.[12] As a result, hackers gained access to sensitive information within the Democratic National Committee's (DNC) emails and servers. Within several months, WikiLeaks gains access to the emails, and publishes them days before the Democratic National Convention. In early October 2016, the Department of Homeland Security links the hacks to Russia. WikiLeaks then publishes a further 58,000 messages over the course of October and November 2016, all from Clinton's chairman John Podesta.[13] Not only did the numerous attacks simply leak documents and emails incriminating Clinton, but the hackers also attacked voting systems in up to 21 states. The hack was largely effective in swaying voters away from Clinton, but they also undermined the fundamental democratic system of a major Western Liberal Democracy. This type of cyberwarfare being used to interfere with another country's political system degrades democratic processes and largely infringes on the privacy of political figures affected. Trump's denial of overt Russian hacking is

[9] https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c065b228eb08

[10] http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

[11] https://www.dni.gov/files/documents/ICA_2017_01.pdf

[12] https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

[13] Ibid.

concerning for the entire international community, especially considering it is widely accepted that the attacks were directly ordered from Putin himself.[14] However, it was also costly for international relations: 35 diplomats were forced to leave the US, and sanctions were placed on 4 Russian individuals and 2 Russian entities. In July of 2018, the US Department of Justice charged 12 Russians with the massive attack. All twelve are members of the Russian Intelligence Agency, also known as GRU.[15] Nevertheless, this hack highlights the fragility of elections against cyberattacks, and raises concerns for the legitimacy and safety of future elections.

Cambridge Analytica

Starting in 2014, the London-based data analytics firm faced worldwide criticism and recently declared bankruptcy as a result of improperly shared data collected from Facebook.[16] The data of an estimated 87 million people was exposed to the firm via a Facebook app, "thisismydigitallife."[17] A loophole in Facebook's Application Programming Interface (API), which allows applications to communicate and transfer information, meant that Cambridge Analytica was able to access the private information of not only those who took the quiz directly, but also the data of the users' friends on Facebook. Moreover, the firm is intricately linked with Donald Trump's 2016 campaign.

Vice President of the firm and former White House Chief Strategist, Steve Bannon, worked alongside conservative donors Rebekah and Robert Mercer to fund Cambridge Analytica. Before being fired in November of 2017, Bannon managed to convince the Trump campaign to hire the firm.[18] Although the effects of the firm's role in the campaign remain unclear in relation to Trump's election, the concerning nature of the firm itself coupled with Facebook's failure to adequately safeguard user data present an interesting case of vulnerability within the digital realm. This is an example of a case where the cybersecurity threat involved is in a grey area of legality, where no explicit attack seemed to have occurred but the damage is undeniable.

WannaCry

Hitting more than 100,000 organizations in 150 countries, the malware known as WannaCry is widely considered the largest extortion attack ever.[19] The key component of the virus takes advantage of Windows systems, encrypts the user's files and demands a payment of $300 in Bitcoin.[20] The estimated

[14] http://time.com/5340060/donald-trump-vladimir-putin-summit-russia-meddling/
[15] https://www.justice.gov/file/1080281/download
[16] https://www.bbc.com/news/technology-43649018
[17] https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram
[18] Ibid.
[19] https://www.cbsnews.com/news/cyberattack-hit-more-than-100000-groups-in-at-least-150-countries-europol-says/
[20] https://www.symantec.com/security-center/writeup/2017-051310-3522-99

costs due to losses hover around 4 billion, according to cybersecurity firm Cyence.[21] The Trump administration has publicly condemned the Lazarus Group, a hacking entity that operates on behalf of the North Korean government, for the attacks. WannaCry was responsible for attacks on Britain's hospitals, Germany's national railway, a major telephone company in Spain, as well as university networks in China. Greatly damaging both digital and physical infrastructure, WannaCry gave security experts a clairvoyant glimpse into the potential for future attacks.[22]

Sony Pictures Hack

In November of 2014, a hacking group who identified themselves as "The Guardians of Peace" (GOP) stole mass amounts of data - reportedly around 100 terabytes - wiped hard drives, and leaked sensitive files to the public.[23] The attack was carried out largely in retaliation for the upcoming release of the satirical movie "The Interview," which centres around the assassination of North Korean leader Kim Jong-Un.[24] The film's release was even canceled due to terrorist threats delivered by the GOP. The US has since concluded that North Korea was "centrally involved" in the attacks, and in 2018, they pressed charges against programmer Park Jin Hyok.[25] The response to the attack was largely unusual: it remains rare for a country like the US to publicly accuse another nation of a cyberattack. Nevertheless, the repercussions of a large-scale cyberattack on a massive corporation like Sony led to the resignation of Chairwoman Amy Pascal, the application of economic sanctions from the US on the DPRK, and degraded trust in the corporation.

Equifax Data Breach

Widely regarded as the largest data breach in history, the Equifax Data Breach resulted in hackers obtaining access to the private information of over 143 million Americans.[26] This breach in particular is so problematic because of the kinds of data and information collected. Due to the stolen Social Security Numbers and credit card information, this hack allows criminals to easily gain access to banks, insurance accounts, and other critical businesses. The Equifax Data Breach is a prime example of the repercussions and backlash caused by cyberattacks that affect corporations. Within the different actors affected by cyberattacks and cybercrime, corporate attacks are often the most damaging to all actors involved, costing millions of dollars in damage, leading to the downfall of the company, exposing millions of individuals' private information, and degrading the trust of the people in that given corporation. Corporate attacks degrade public trust in data collection and privacy, and often lead to major backlash against these companies, with users turning away from corporations who have failed to protect their privacy. As a result, security measures increase and more disclaimers are put out - but even despite this,

[21] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
[22] Ibid.
[23] http://time.com/3639275/the-interview-sony-hack-north-korea/
[24] https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0
[25] https://www.cnn.com/2018/09/06/politics/doj-sony-hack-charges/index.html
[26] https://www.cnbc.com/2018/03/10/in-the-wake-of-the-equifax-data-breach-consumers-more-at-risk.html

consumers are constantly put at risk due to the increasingly invasive nature of cybercrime. As opposed to attacks on the individual, hackers can gain access to a large database of information in one fell swoop, with millions of accounts located conveniently in one database. A weakness in the tool used to design web applications, also known as the Apache Struts flaw, was found months before hackers actually exploited the software.[27] The company received major backlash for waiting to release information on the hack until after a month after it learned of the attacks. The disparity and lack of transparency between companies and their users only highlights the flaws with mass data collection; ensuring user privacy and security is a constant race against hackers.

Data Element Stolen	Standardized Columns Analyzed	Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

Chart outlining critical information obtained from the Equifax Data Breach.[28]

United Nations Involvement

The United Nations has long recognized the importance of security in cyberspace. Consequently, several resolutions have been adopted over the years to address cybersecurity and cyberwarfare. Notably, these include:

A/RES/57/239 (2003)
Creation of a global culture of cybersecurity

[27] https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html
[28] https://www.thesslstore.com/blog/equifax-data-breach-total-data-lost-the-final-count/

This resolution served as a preliminary step for delegations to become aware of the threat posed by unguarded cyberspace. The resolution centers around awareness and responsibility and is fitting for the novelty surrounding technology used for cyberattacks at the time. Its main purpose was to call on countries to develop an awareness surrounding cybersecurity, and therefore was largely symbolic rather than tangibly functional. It provided a brief framework of 9 complementary elements to ensure security. The framework served the simple purpose of introducing cybersecurity into a global narrative of regulation and prevention.

A/RES/64/211 (2009)

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

Focusing on safeguarding critical infrastructure, the resolution encompasses several aspects critical to maintaining cybersecurity: situational assessment, outlining roles and responsibilities, and attack management and recovery. It focuses heavily on the importance of assessment as a preliminary step to prevent cyber attacks, and also delegates responsibilities to the main actors in this topic: the federal government, local/regional governments, non-government actors (institutions, academia, industries, etc.), and individual citizens. The resolution also covers the legal frameworks that govern cybersecurity.

Budapest Convention on Cybercrime

Established by the Council of Europe on November 23rd, 2001, the Budapest Convention is the only multilateral legally binding instrument surrounding cybercrime.[29] Although the Convention does not concern cyberwarfare per se, it is still the only legally binding framework in existence surrounding the malicious use of information technology. The convention entered into force in July 2004, and as of 2018, 57 delegates had ratified the convention.[30]

Secretary-General's Remarks on Cyber Warfare

On February 19th, 2018, Secretary-General Antonio Guterres called for clearer global regulation surrounding cyberwar. He questioned where cyberwar fit within international regulation, stating that "*episodes of cyber warfare between states already exist [...] there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it*".[31] He touched on the devastating effects of cyberattacks on critical infrastructure, such as power grids and electrical networks. However, his speech left several crucial questions unanswered. Regarding his call for additional regulation surrounding cyberwarfare, many were unsure as to why "r*ules specifically*

[29] https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf

[30] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

[31] https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-id USKCN1G31Q4

developed for cyber warfare would fare any better than other rules of international law designed to apply in times of war".[32] This is also a highly contested area of debate, raising questions around the effectiveness and efficacy of legal frameworks pertaining specifically to cyberwar.

Seeking Resolution

International Multilateral Treaty

A resolution that has been proposed multiple times, the establishment of a multilateral, international, binding legal framework presents itself as a logical next step to effectively secure cyberspace. Currently, there is no active treaty for cyberwarfare, and there is often confusion about how cyber attacks fit into existing international frameworks. The Secretary-General, having already called for the establishment of one such treaty, justly highlighted the confusion around how international humanitarian law regulates cyberattacks. Therefore, the establishment of an international multilateral treaty would act as an independent binding framework to govern matters of cybersecurity and cyberwarfare. However, this solution is not without opposition. It remains unclear whether or not a new treaty would actually be needed, as it would be redundant to create yet another binding piece of international legislation when simple adjustments to existing frameworks (like the Budapest Convention on Cybercrime and the Tallinn Manual) are a viable option.

Increased Security

This solution takes place on two levels: on the larger governmental and corporate levels, as well as the individual micro level. In terms of the latter, governments and corporations should work to secure their information and make cybersecurity a priority. Establishing a branch of government dedicated solely to cybersecurity, funding more initiatives dedicated to securing cyberspace; these are all viable options for governments to take in order to secure critical infrastructure. At the same time, transparency and honesty is needed to ensure that users' rights and privacy are being protected. The same can be said for individuals: rudimentary protection against malware and basic integration of information about internet safety (netiquette) is sorely needed to combat cyber warfare on an individual level. Working in tandem, the combination of individual and government/corporate cooperation is an effective measure to preserve cybersecurity. However, the increasing ease with which individuals are able to attack others constantly undermines efforts to secure cyberspace. Due to factors like speed, visibility, and heavy reliance on the internet, it is extraordinarily difficult to properly secure cyberspace, which raises questions about how effective increasing security actually is. The rapidly evolving technology employed by hackers makes it hard for civilians and corporations to deal with them accordingly. Although these measures will do little in terms of defending against a major attack on infrastructure, it is enough to mitigate some of the harms seen by smaller attacks.

[32] https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers

Regulating Cyberspace

Controversial yet successful, the idea of regulating cyberspace and the internet to counter against a cyberattack is an area of heated debate. As with physical surveillance, governments may choose to monitor internet activity for certain individuals, or even gather personal information through cyberspace in pursuit of finding criminals. Is it justified for the government to infringe on rights to privacy with data collection and internet activity in the name of cybersecurity? A controversial variation on traditional regulation is the idea of a "kill switch". A prime example of an effective kill switch against malware was MalwareTech's success against the WannaCry ransomware attacks in May of 2017. Freezing institutions, companies, and even UK's National Health Service, WannaCry was defeated by a simple kill switch embedded in its system.[33] A kill switch is, simply put, a switch that kills all internet traffic. Terminating access to the internet as both a preventative and retaliatory measure, this would be relatively effective against domestic cyberattacks. However, the implications of shutting off millions from internet access poses a large moral dilemma. Is it justified to infringe upon the freedom of millions of civilians to access information and services to prevent against a cyberattack?

Bloc Positions

United States of America

With a budget request of $647 million for the 2018 fiscal year, the US Cyber Command (USCYBERCOM) is a major component of American defense. It is a major superpower in terms of military might, and its prowess with cyberwar proves to be no different. A victim of recent cyber attacks, it is no stranger to being involved in attacks in cyberspace. However, it is clear that the US will take every measure necessary to protect its infrastructure and people. They will undoubtedly match every move in the global race for domination over cyberspace. Nevertheless, they are a staunch supporter of diplomatic solutions as well, favouring an international multilateral treaty in tandem with increased security.

Russian Federation

One of the most powerful major players in the world of cyberwarfare, Russia has constantly proved itself to be a dangerous enemy and powerful ally. Russian hackers and malware have wreaked havoc on Estonia, France, Georgia, Germany, Kyrgyzstan, Ukraine, and the US, though evidence indicting Russia as the culprit is sparse. [34][35][36][37][38] Furthermore, tightly controlling the internet, and supporting a kill

---

[33] https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/
[34] https://www.bbc.com/news/39655415
[35] https://www.bbc.com/news/technology-37590375
[36] https://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/
[37] https://www.aljazeera.com/news/2016/12/bfv-russia-destabilise-germany-161208141856179.html
[38] https://www.wsj.com/articles/SB123310906904622741

switch, may be within Russia's sovereign interests to regulate cyberspace. However, Kremlin support for a multilateral treaty and international cooperation may be somewhat lacking. Considering the geopolitical tensions in the present day, Russia will undoubtedly have an interest in expanding its cyber arsenal.

China

With China's tight censorship and its notorious "cybersecurity" law, China is another major superpower in the world of cyberwarfare. There has been a notable downward trend in the frequency and severity of attacks alleged to have originated from China ever since the 2015 agreement between the US and China to "*agreed not to conduct or knowingly support economic cyber-espionage*".[39] This has proved to be a monumental agreement between the two superpowers, and points to a bright future for China's future in the international community. Nevertheless, Chinese aggression in its attacks elsewhere should not be disregarded. As a heavily controlling government cracks down on internet freedom, this delegate should be ready to represent the dichotomy of diplomacy and belligerence China consistently demonstrates.

Iran

Iranian cyberspace has been host to some of the world's most costly and consequential attacks. An emerging power in cyber warfare, Iran has seen both sides of these attacks, having played both victim and predator in recent history. Victim to the Stuxnet worm in the early 2000s, they experienced firsthand the devastation of malicious software.[40] A decade later, Iran's cyber capacities are masked by proxies, covertly carried out, and devastatingly successful. Tehran has used cyberwarfare to retaliate against the US and Saudi oppression, and consistently conducts espionage to gather intelligence.[41] Guerrilla attacks are quite frequent, often stemming from individuals "defacing" websites with pro-Iran messages, defending their beliefs and attacking those believed to be opposition.[42] Although they employ simpler hacking techniques and less sophisticated weaponry, they have found success in attacking unsecured US banks, Saudi oil companies, and opposing governments. Tehran's ability to conduct these attacks stands as a retaliatory sign of strength - though Iran is still developing its cyber arsenal, it remains a force to be reckoned with.

North Korea

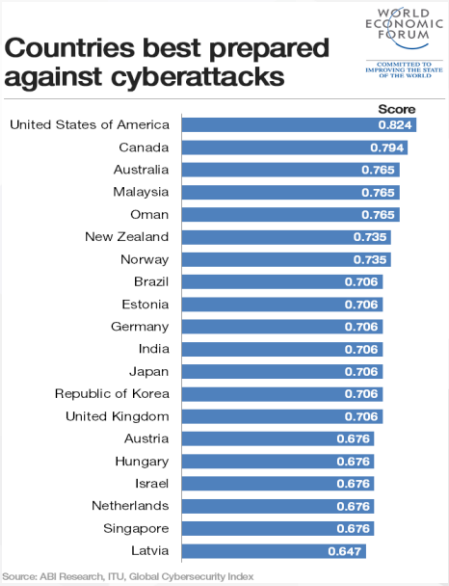
For some, North Korea's cyber arsenal may be even more fearsome than its nuclear arsenal. Increasingly powerful and incredibly effective, North Korea's cyberwarfare is capable of stealing state secrets, siphoning millions of dollars from banks, and its state-sponsored attacks rival those of any Western nation. Reportedly affiliated with the Lazarus Group (behind the WannaCry attacks), they have proved to

[39] https://www.cnn.com/2016/09/29/asia/china-cyber-spies-hacking/index.html
[40] Ibid.
[41] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-introduction-pub-75138
[42] https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427

be successful in their large-scale attacks against various cryptocurrencies, international banks, Sony, and their enemies' governments.[43] Their rapid development is extremely impressive considering the restrictive nature of the North Korean government - despite most citizens only being able to access a heavily censored, state-run internet, they have nonetheless produced some of the most formidable hackers and attacks in the history of cyber warfare. North Korea's willingness to comply with any proposed legal frameworks may be an issue, and all delegates should keep working towards universal solutions that incorporate as many states as possible; even considering highly restrictive states like the DPRK.

Other Western Liberal Democracies (WLD)

Countries with general Western ideologies (e.g. the United Kingdom, Japan, South Korea, Germany, France) all hold similar stances on cyber warfare. Valuing diplomatic action and peaceful resolution above all else, these countries will protect citizens' freedoms valiantly. Solutions like the kill switch are unlikely to resonate well with these countries, and would only be considered as a last resort. With the funds and resources necessary to safeguard information and technology, WLDs can choose to either take on an observer role, or participate more actively in conflict, depending on regional opinion. They have quite a bit of choice over their actions and foreign policy, but will ultimately prioritize a peaceful solution.



The World Economic Forum's ranking on preparedness against cyberattacks, measured using a variety of factors (i.e regulations, policies, national strategies, awareness raising, and cooperative partnerships) that determine preparedness in defence and retaliation.[44][45]

[43] https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html
[44] https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/
[45] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Discussion Questions

1. What constitutes an act of cyberwar?
2. What different courses of actions should be pursued in instances of guerilla and state-supported attacks? Should they differ, or follow the same framework?
3. Under what circumstances should collective state retaliation (i.e sanctions, tariffs, engagement in war) take place? Is it ever justified?
4. How does your delegation balance internet freedom with internet surveillance?
5. What are steps to take in order to secure critical infrastructure against large scale attacks?
6. Where should the line be drawn in terms of UN intervention in cyberwar?
7. How should we best regulate cyberspace internationally?
8. How does the international community best combat state-supported cyber warfare without escalating into full blown war?

Further Reading

Center for Strategic & International Studies
A comprehensive list of major cyber attacks since 2006.
https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

The Regulatory Review (University of Pennsylvania)
Overview on regulatory frameworks concerning cyberwarfare.
https://www.theregreview.org/2017/01/13/kang-regulating-international-cyberwarfare/

International Committee of the Red Cross
Discusses the Tallinn Manual, as well as provides a general overview on cyber warfare.
https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

The Guardian - Cyberwar
Provides convenient access to latest updates and articles on cyberwar.
https://www.theguardian.com/technology/cyberwar

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
Outlines the legal frameworks and international law surrounding cyber attacks and cyber warfare.

Works Cited

CSIS. “Significant Cyber Incidents Since 2006.” *Center for Strategic and International Studies*, 2018, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

The Economist. “A Spook Speaks.” *The Economist*, 30 June 2012, www.economist.com/business/2012/06/30/a-spook-speaks.

General Assembly resolution 57/239, Creation of a global culture of Cybersecurity, A/RES/57/239 (31 January 2003), available from undocs.org/A/RES/57/239.

General Assembly resolution 64/211, Creation of a global culture of Cybersecurity and taking stock of national efforts to protect critical information infrastructures , A/RES/64/211 (17 March 2010), available from undocs.org/A/RES/64/211.

General Assembly resolution 70/237, Developments in the field of information and telecommunications in the context of international security, A/RES/70/237 (30 December 2015), available from undocs.org/A/RES/70/237.

Kang, Alex. “Regulating International Cyberwarfare.” *The Regulatory Review*, 28 Mar. 2017, www.theregreview.org/2017/01/13/kang-regulating-international-cyberwarfare/.

Kelty, Christopher M. “The Morris Worm.” *Limn*, 26 Jan. 2018, limn.it/articles/the-morris-worm/.

Khalip, Andrei. “U.N. Chief Urges Global Rules for Cyber Warfare.” *Reuters*, 19 Feb. 2018, www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

Lee, Timothy B. “How a Grad Student Trying to Build the First Botnet Brought the Internet to Its

Knees." *The Washington Post*, 1 Nov. 2013, www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.67902da3ba2c.

Mallet, Victor. "Financial Times Mutually Assured Destruction in Cyberspace." *Financial Times*, 20 Aug. 2008, www.ft.com/content/ca5cb050-6eb7-11dd-a80a-0000779fd18c.

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*, 12 Aug. 2008, www.nytimes.com/2008/08/13/technology/13cyber.html.

Markoff, John. "Vast Spy System Loots Computers in 103 Countries." *The New York Times*, 28 Mar. 2009, www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, 27 Apr. 2017, www.bbc.com/news/39655415.

Menn, Joseph. "Financial Times Cyberattacks Penetrate Military Secrets and Designs." *Financial Times*, 3 Aug. 2011, www.ft.com/content/d4f09016-bda3-11e0-babc-00144feabdc0.

O' Harrow, Robert, and Greg Linch. "Timeline: Key Events in Cyber History." *The Washington Post*, 3 June 2012, www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/.

O'Flaherty, Kate. "Cyber Warfare: The Threat From Nation States." *Forbes*, 3 May 2018, www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/.

Santiago, José, and World Economic Forum. "Top Countries Best Prepared against Cyberattacks." World Economic Forum, www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/.

Seglins, Dave. "CSIS Chief Warns of Cyberattack Threat to Canada's Infrastructure" *CBCnews*, 19

Nov. 2015, www.cbc.ca/news/canada/csis-cyberattack-michel-coloumbe-1.3325531.

Thornburgh, Nathan. “Inside the Chinese Hack Attack.” *Time*, 25 Aug. 2005, content.time.com/time/nation/article/0,8599,1098371,00.html.

Wagner, Daniel. “Cyberwarfare Against Critical Infrastructure.” *International Policy Digest*, 25 Mar. 2018, intpolicydigest.org/2018/03/25/cyberwarfare-against-critical-infrastructure/.