OSCE Study Guide

The Issue of Cyber Warfare

FireEye
Subscribe to FireEye Alerts
[X] NEW ATTACK: FROM [GERMANY] TO [KOREA, REPUBLIC OF]
[X] NEW ATTACK: FROM [UNITED STATES] TO [SAUDI ARABIA]
[X] NEW ATTACK: FROM [SAUDI ARABIA] TO [KOREA, REPUBLIC OF]
[X] NEW ATTACK: FROM [UNITED STATES] TO [TURKEY]
CYBER THREAT MAP
LOCAL TIME
15:10:22
ATTACKS TODAY
30,125
ATTACKERS
TARGETS
TOP 5 REPORTED INDUSTRIES
EDUCATION
ENERGY/UTILITIES
HIGH-TECH
GOVERNMENT: FEDERAL
GOVERNMENT: STATE & LOCAL
UNCLASSIFIED
DELL

osce

PREPMUN 2022

Table of Contents

OSCE

Introductions

Welcome letter
Chair introductions
Council introduction

Welcome Letter

Dear delegates,

Welcome to the Organisation for Security and Cooperation in Europe (OSCE) of PREPMUN’22. As delegates from different member states convene, it is unavoidable for them to discuss the increasing threat of cyber warfare in today’s technological age.

The issue of cyber warfare has gained traction in recent years as countries aim to bolster their national cyber defence and invest in offensive cyber capabilities. The issue has certainly evolved as technology becomes more advanced over the years. Notwithstanding the varying stances of each member state, OSCE hopes that delegates can come together on a united front when discussing issues related to the topic at hand.

Debate in council will cover several aspects of the multifaceted issue of cyber warfare, from the legalities of cyber warfare to the proliferation of malware and offensive cyber capabilities. As a Dais, we look forward to your active participation and contribution to rigorous debate and erudite solutions despite the contentious nature of this topic. Most importantly, we hope that you can have fun and make lasting friendships with other delegates as you journey through PREPMUN’22!

Yours Truly,

The Dais of the OSCE

Chen Ying, Daniel and Seng Hao

Chair Introductions

Head Chair: Chen Ying

Chen Ying is a lover of food, purple (yes the colour) and of course, MUN. As an avid reader, Chen Ying spends most of her time reading or finding new books to read. Being a creature of habit, she often eats the same dish everytime she goes to a restaurant and has put in a significant amount of effort to eat a greater variety of dishes. The same way that she has stepped out of her comfort zone, Chen Ying hopes that delegates will step out of their comfort zone and grow as both a speaker and a MUNner during PREPMUN 2022.

Deputy Chair: Daniel Adam

Daniel used to have weird life goals like visiting every MRT station in Singapore and pulling an all-nighter thrice a month. Now, he just uses whatever time is left from his hectic daily schedule (bombarded with lessons, council events, and of course, MUNs) to indulge in activities he loves, such as ice skating, jogging, badminton, and ultimate frisbee. Oh yes! Fun fact: Daniel hates eggs with a burning passion. Daniel hopes that his delegates will make new friends and gain a fruitful council experience at PREPMUN 2022.

Deputy Chair: Kuek Seng Hao

Seng Hao loves to sleep, watch netflix and sing spontaneously during biology lessons. He is thrilled to be chairing OSCE and wishes for delegates to take PREPMUN’22 as an opportunity to become more confident and eloquent speakers, as well as to forge meaningful friendships with fellow delegates.

Council Introduction

Mandate and Purpose of the Council

The Organisation for Security and Cooperation in Europe (OSCE) deals with security in Europe, encompassing four main dimensions: the politico-military, economic, environmental, and human dimension.[1] OSCE tackles problems arising from all four dimensions, from arms control and policing to non-war related issues such as protecting minority rights and ensuring the sustainable use of natural resources. Often, the council also deals with cross-dimensional issues such as migration and cybersecurity.[2] In the OSCE, all 57 participating member states have equal status, and decisions are made only when a consensus is reached, though on a not legally binding basis.[3]

History and Milestones

The OSCE was created during the Cold War détente of the early 1970s, and was initially named the Conference on Security and Cooperation in Europe (CSCE).[4] Up until 1990, the CSCE mainly consisted of a series of meetings and conferences that built on the commitments that the member states had made in previous meetings, while periodically reviewing the implementation of policies. In the Charter of Paris for a New Europe, the CSCE was called upon to help manage the historic change that was happening in Europe as well as respond to the new challenges of the post-cold war period. As part of the process of the institutionalisation of CSCE, CSCE was renamed to OSCE in December 1994.[5]

[1] Claus Neukirch, "OSCE | Organization for Security and Co-Operation in Europe," Organisation for Security and Co-operation in Europe, December 31, 2010, https://www.osce.org/whatistheosce.

[2] Claus Neukirch, "OSCE | Organization for Security and Co-Operation in Europe," Organisation for Security and Co-operation in Europe, December 31, 2010, https://www.osce.org/whatistheosce.

[3] Claus Neukirch, "OSCE | Organization for Security and Co-Operation in Europe," Organisation for Security and Co-operation in Europe, December 31, 2010, https://www.osce.org/whatistheosce.

[4] "History," Organisation for Security and Co-operation in Europe, accessed July 31, 2022, https://www.osce.org/who/87.

[5] "History," Organisation for Security and Co-operation in Europe, accessed July 31, 2022, https://www.osce.org/who/87.

OSCE

The Issue of Cyber Warfare

Topic Introduction

In this digital age, most people have access to the Internet and various forms of technology. While this interconnectivity has brought incalculable benefits, it has opened the world up to another form of vulnerability. In recent years, terrorist organisations and even state actors have greatly developed their cyber attack capabilities, launching attacks ranging from ransomware to denial-of-service operations. With the instances of cyber espionage increasing, classified and sensitive information is also left vulnerable and susceptible to attack in cyberspace. According to Forbes, the average number of cyber attacks and data breaches in 2021 increased by 15.1% from the previous year,[6] showing how cyber attacks and data breaches are growing increasingly common.

As our world becomes increasingly intertwined with cyberspace, with trade networks, emergency services, basic communications and other activities taking place in cyberspace, the risks of cyber attacks will only increase. In fact, the destructive capabilities of cyber warfare might soon equal physical warfare. Cyber attacks can be used to cause disruption to activities within a state, be it transportation, water, defence, fuel or communications. For example, Stuxnet, the first credited cyber attack, was used to disable the computers that operated uranium-enriching centrifuges in Natanz, Iran, hence disrupting its military infrastructure.[7]

As most states now store their information digitally, technology infrastructure has also been a key target for cyber espionage and attacks. The infiltration of such systems could risk the physical safety of people, economic security of a country and even national public health systems.[8] For example, in the United States, relentless cyber attacks targeting hospitals in 2021 put financial stress on the nonprofit hospitals and health systems, which could risk the physical health of people who do need these services.[9] The dangers of cyber warfare blurs the lines between cyber warfare and traditional, physical warfare with many countries not fully adjusted to these new threats yet.

[6] Chuck Brooks, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," Forbes, June 3, 2022, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/.

[7] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired. Wired, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[8] Brijesh Singh, "India's Cybersecurity and Its Impact on the Economy," Gateway House (blog), August 4, 2022, https://www.gatewayhouse.in/indias-cybersecurity-and-its-impact-on-the-economy/.

[9] Heather Landi, "Relentless Cyberattacks Are Putting Financial Pressure on Hospitals: Fitch Ratings," Fierce Healthcare, July 26, 2021, https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings.

Background

Definitions

Cyber warfare: Currently, there is no authoritative definition of the term "cyber warfare". However, in the International Humanitarian Law (IHL), cyber warfare often refers to "operations against a computer or a computer system through a data stream when used as a means or method of warfare in the context of an armed conflict".[10]

Cyber attack: refers to an attack launched by cybercriminals using a single or multiple computers against one or more computers and networks.[11] There are many types of cyber attacks. Some of them include espionage, sabotage, denial-of-service (DoS), electrical power grid attacks, propaganda attacks, economic disruption, and surprise attacks, though the list is non-exhaustive.[12]

Offensive Cyber Capabilities (OCCs): refers to the combination of various variables such as technologies, people and organisations that jointly allow for offensive cyber operations to be carried out.[13]

Information Communication Technologies (ICTs): refers to the combination of diverse technological tools and resources which are mainly used for telecommunication and the sharing, storage as well as creation of information.[14]

Malware or "malicious software": refers to software that is specifically designed with the intention to disrupt, damage, or gain unauthorised access to a computer system.[15]

[10] "International Humanitarian Law," International Committee of the Red Cross (International Committee of the Red Cross), accessed August 1, 2022, https://www.icrc.org/en/download/file/40569/en_-_handbook_humanitarian_law_-_web.pdf.

[11] "What Is a Cyber Attack?," Check Point Software, accessed August 1, 2022, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

[12] "What Is Cyber Warfare | Types, Examples & Mitigation | Imperva," Learning Center (blog), August 18, 2021, https://www.imperva.com/learn/application-security/cyber-warfare/.

[13] Florian Egloff and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," Oxford Academic (Oxford Academic, October 26, 2021), https://academic.oup.com/jogss/article/7/1/ogab028/6412386.

[14] "Information and Communication Technologies (ICT) | Unesco IIEP Learning Portal," UNESCO International Institute for Educational Planning (UNESCO International Institute for Educational Planning), accessed August 1, 2022, https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict.

[15] "Malware, Trojan, and Spyware – Information Security," California State University, Chico (California State University, Chico), accessed September 15, 2022, https://www.csuchico.edu/isec/stories/malware-trojans-spyware.shtml.

Critical infrastructure: refers to infrastructure vital for the security, national economic security, national public health or safety of a country.[16] This includes energy sectors, health sectors, finance sectors, agricultural sectors, and other kinds of sectors crucial in ensuring the sustainability of a country.

History

The first cyber attack occurred in 2010. Stuxnet, a computer worm, infiltrated and disable computers that operated uranium-enriching centrifuges in Natanz.[17] Stuxnet was credited as the first cyber attack to showcase a cyber weapon's capability to directly impact physical systems and processes.[18]

Stuxnet showed that there were many organisations and nations actively developing offensive cyber capabilities (OCCs) with the purpose of disrupting important national infrastructures. The fact that cyber warfare could inflict real-world damage in the form of destroying public infrastructure and taking lives brought a sense of urgency to global Industrial Control System (ICS) and Operational Technology (OT) communities, raising awareness regarding the possibility of cyber warfare as a legitimate form of warfare one day and acting as the catalyst for developments of and improvements to cybersecurity measures. After becoming publicly available, Stuxnet also provided a platform and blueprint for future cyber attacks to cybercriminals and terrorists, paving the way for future cyber threats.

Since then, various countries have taken action to bolster their national security against the threat of cyber warfare. For example Iran has strengthened their cyber capabilities through investing in cybersecurity developments, such as the Iran Cyber Police and Supreme Council of Cyberspace.[19][20] Besides this, Stuxnet has also prompted nations to strengthen their defence by implementing preventive policies and measures against cyber offensive operations.[21] Though there are no official laws governing the use of cyber warfare, international bodies and humanitarian organisations such as

[16] "Critical Infrastructure Sectors | CISA," Cybersecurity & Infrastructure Security Agency (Cybersecurity & Infrastructure Security Agency, October 21, 2020), https://www.cisa.gov/critical-infrastructure-sectors.

[17] Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Stanford (Stanford, 2011), http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.

[18] "Stuxnet - The First Cyber Weapon," Gemserv (Gemserv, December 31, 2019), https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/.

[19] Andrea Shalal-Esa, "Iran Strengthened Cyber Capabilities after Stuxnet: U.S. General," Reuters, January 18, 2013, sec. Technology News, https://www.reuters.com/article/us-iran-usa-cyber-idUSBRE90G1C420130118.

[20] "Iranian Offensive Cyber Attack Capabilities" (Congressional Research Service, January 13, 2020), https://sgp.fas.org/crs/mideast/IF11406.pdf.

[21] Adam Segal, "Cyber Conflict After Stuxnet," Council on Foreign Relations (blog), June 27, 2016, https://www.cfr.org/blog/cyber-conflict-after-stuxnet.

the International Committee of the Red Cross have also applied the principles of International Humanitarian Law to cyber warfare.[22]

In the past, the UN has also discussed the matter of cyber warfare. In 2021, the UN cybersecurity Open-Ended Working Group (OEWG) released a consensus report containing recommendations for advancing peace and security in cyberspace.[23] This further solidifies past progress made on the issue of cyber warfare, and could also enable a greater degree of accountability for malicious state behaviour in cyberspace. Besides this, the UN has also previously endorsed multiple resolutions relating to cybersecurity and combating cyber threats.[24]

Key Issues

The Increasing Prevalence of Cyber Attacks

Cyber attacks are becoming more prevalent both within and between states. Cyber attacks have globally increased by 15.1% from 2020 to 2021, and are only becoming more prevalent, with each attack having a significantly large impact.[25] In July 2022, hackers temporarily took down websites belonging to the Albanian Prime Minister's Office and the Parliament, and the e-Albania portal used to access public services.[26] The vital government services that Albanians rely upon, from healthcare to tax have all been affected, with significant consequences for vulnerable people.[27]

Cyber attacks are not only prevalent within a state but are also common between states. Attacks on Ukrainian government websites (by Russia) in January 2022 occurred, one day after US-Russian negotiations on Ukraine’s future in NATO failed. In February 2022, Russia also took down several

[22] “Cyber Warfare: Does International Humanitarian Law Apply?,” February 15, 2021, https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.

[23] Josh Gold, “Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?,” Council on Foreign Relations, March 18, 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

[24] “UN Resolutions,” ITU, accessed October 31, 2022, https://www.itu.int:443/en/action/cybersecurity/Pages/un-resolutions.aspx.

[25] Chuck Brooks, “Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know,” Forbes, June 3, 2022, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/.

[26] Chuck Brooks, “Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know,” Forbes, June 3, 2022, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/.

[27] Richard Speed, ‘Albanian Government Websites Go Dark after Cyberattack’, accessed 31 October 2022, https://www.theregister.com/2022/07/18/albania_down/.

major Ukrainian governmental and banking websites.[28] Thus, the increasing prevalence and potency of cyber attacks, has resulted in Cyber Attacks becoming an increasing threat for all countries.

Political Subterfuge

Countries may also exploit cyberspace to undermine other countries. To date, there have been a multitude of cyber attacks launched in a bid to inflame existing discontent in nations. During the 2016 US presidential election, a wide-ranging group of Russian hackers exploited a number of loopholes in voter databases, targeting voter registration systems and state websites. There were also audacious attempts to hack the Hillary Clinton campaign, the Democratic Congressional Campaign Committee and the Democratic National Committee, as well as the campaign of Sen. Marco Rubio.[29] This sewed a lot of distrust in American democracy as the credibility of the election was undermined. While many already doubted that the election was rigged, a cyber attack only compounded the issue further, causing many to be discontented with the security of voter registration systems and the management of the election as a whole. Similar attempts were made in 2020, when Microsoft speculated that Biden's presidential campaign was specifically targeted by Russian hackers via insidious phishing attacks against the communications advisors of the campaign, SKDKnickerbocker.[30] Though unsuccessful, this shows that state attempts to meddle in foreign affairs through cyber espionage still persists and remains a threat to the political stability of countries worldwide. If left unchecked, cyber attacks aimed to undermine other countries will only increase in frequency.

Attacks on Government Systems and Databases

Attacks on government systems and databases can result in classified information that relate to the strategic interests of a country being compromised. In 2020, a major cyber attack committed by a Russian state-sponsored group penetrated thousands of organisations globally including the United States federal government, leading to a series of data breaches.[31] The cyber attack and data breaches were reported to be among the worst cyber-espionage incidents the U.S. ever experienced. More than 200 organisations around the world had been reported to be affected by the attack, including NATO,

[28] Jakub Przetacznik, "Russia's War on Ukraine: Timeline of Cyber-Attacks | Think Tank | European Parliament," European Parliament, June 21, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549.

[29] Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," Time (Time, April 18, 2019), https://time.com/5565991/russia-influence-2016-election/.

[30] Joel Schectman et al., "Exclusive: Microsoft Believes Russians That Hacked Clinton Targeted Biden Campaign Firm - Sources," Reuters, September 10, 2020, sec. Banks, https://www.reuters.com/article/us-usa-election-cyber-biden-exclusive-idUSKBN2610I4.

[31] Ryan Gallagher and Kitty Donaldson, "Bloomberg - Are You a Robot?," December 14, 2020, https://www.bloomberg.com/news/articles/2020-12-14/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack.

the U.K. government, the European Parliament, and Microsoft.[32] Through manipulation of software keys, hackers were able to access the email systems used by the Treasury Department's highest-ranking officials. This meant that hackers gained access to information regarding economic sanctions that were not yet implemented.[33] In 2018, the SingHealth cyber attack sent shockwaves throughout Singapore. Hackers infiltrated the databases of SingHealth, the largest group of healthcare institutions. The personal particulars of 1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong, were stolen.[34] A government data breach can lead to a major financial loss. According to the Cost of a Data Breach Report 2021, a total average data breach cost of $1.93 million.[35] Apart from the financial losses, data breaches affect the privacy of citizens and reduce the trust that citizens have in their government.

Attacks on Critical Infrastructure

A common trait of typical interstate cyber attacks is the targeting of critical infrastructure. This can include infrastructure owned by non-governmental organisations or global corporations. In 2015, Anthem Inc., a health insurance provider, revealed that anonymous hackers had infiltrated a database with over 80 million records of patients.[36] Anthem also claimed that hackers had stolen private data belonging to tens of millions of current and former customers and employees. With factories across various industries today still running on highly vulnerable operating systems, such as Windows 7 or Windows XP, it is easier for hackers to discover and attack security loopholes.[37] The Colonial Pipeline Ransomware incident in May 2021, which involved a ransom of $4.4 million, is testimony to how much cyber attackers earn from targeting critical infrastructure. Thus, the vulnerability of existing systems, coupled with the profit cyber criminals can make, has made cyber attacks on critical infrastructure all the more alluring.

[32] David E. Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," The New York Times, December 15, 2020, sec. U.S., https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[33] David E. Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," The New York Times, December 15, 2020, sec. U.S., https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[34] Irene Tham et al., "Singapore's Worst Cyber Attack: How It Unfolded," The Straits Times (The Straits Times, July 20, 2018), https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

[35] Rep. *Cost of a Data Breach Report 2021*. IBM, 2021

[36] Reuters Staff, "Anthem to Pay Nearly $40 Million to Settle Data Breach Probe by U.S. States," Reuters, September 30, 2020, sec. U.S. Legal News, https://www.reuters.com/article/us-anthem-cyber-idUSKBN26L2PW.

[37] Jowi Morales, "Why Hackers Target Critical Infrastructure and Why It's Difficult to Upgrade Cybersecurity," MUO, May 7, 2022, https://www.makeuseof.com/why-hackers-target-critical-infrastructure/.

To compound the issue further, hackers also tend to target critical infrastructure owned by the government to inflict more damage on the adversary state during armed conflicts.[38] Cyber attacks during an armed conflict impede civilians from seeking medical help and hamper industries from providing the people with daily necessities. Prior to the Russo-Ukrainian war, a group of Russian cyber criminals referred to as "FIN12" had been expanding hacking operations and targeting the Ukrainian healthcare industry with ransomware attacks.[39] Countries can exploit cyberspace as a strategic military weapon during a war, undermining the distribution of medical goods, food supplies and relief supplies. During the war, Ukraine's public, energy, media, and financial sectors suffered from the incessant cyber attacks. If proven to be successful, these cyber attacks can also block off access to basic services to data theft and disinformation.[40] While countries have made attempts to hold these cybercriminals accountable, these attempts are often fruitless as cyber criminals exploit proxy servers to hide their location evading detection by routing their communication channels through various countries.[41] Therefore, with technology becoming increasingly sophisticated, coupled with the veil of anonymity that cyber criminals enjoy, it is clear that the ramifications of cyber warfare are far-reaching and have to be addressed.

The Proliferation of Offensive Cyber Capabilities (OCCs)

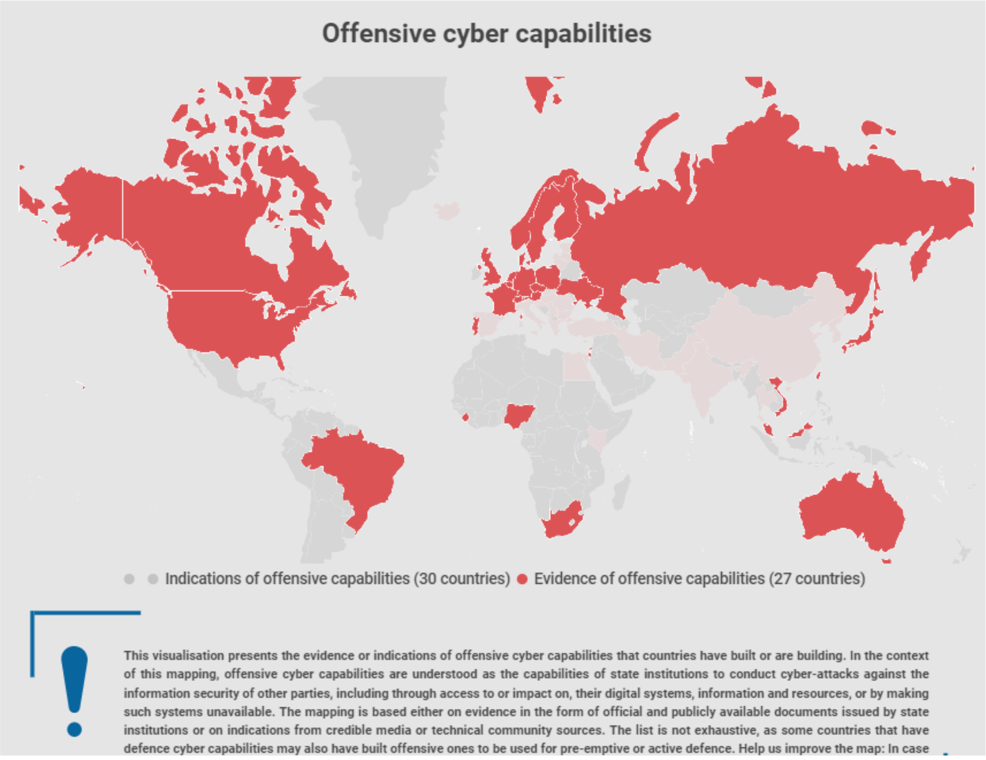
With advanced technology, many countries have started building more cyber weapons and establishing significant amounts of budget for the expansion of their military cyber capabilities. This leads to the proliferation of OCCs as countries compete in a new type of arms race, a race to develop the most advanced OCCs in cyberspace to threaten other unfriendly countries. In fact, 27 countries have a significant number of OCCs. (Figure 2a.)

[38] James Andrew Lewis, "Cyber War and Ukraine," Center for Strategic & International Studies (Center for Strategic & International Studies, June 16, 2022), https://www.csis.org/analysis/cyber-war-and-ukraine.

[39] Nicole Sganga, Catherine Herridge, and Musadiq Bidar, "Foreign Hacking Group Targets Hospitals, Clinics with Ransomware Attacks, Says New Report," CBS News (CBS News, October 7, 2021), https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups/.

[40] Jakub Przetacznik, "Russia's War on Ukraine: Timeline of Cyber-Attacks | Think Tank | European Parliament," European Parliament, June 21, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549.

[41] https://us.norton.com/blog/emerging-threats/how-do-cybercriminals-get-caught


Offensive cyber capabilities
● ● Indications of offensive capabilities (30 countries) ● Evidence of offensive capabilities (27 countries)

This visualisation presents the evidence or indications of offensive cyber capabilities that countries have built or are building. In the context of this mapping, offensive cyber capabilities are understood as the capabilities of state institutions to conduct cyber-attacks against the information security of other parties, including through access to or impact on, their digital systems, information and resources, or by making such systems unavailable. The mapping is based either on evidence in the form of official and publicly available documents issued by state institutions or on indications from credible media or technical community sources. The list is not exhaustive, as some countries that have defence cyber capabilities may also have built offensive ones to be used for pre-emptive or active defence. Help us improve the map: In case

Figure 2a: A diagram representing the distribution of offensive cyber capabilities around the world.[42]

Most of the time, countries purport the primary reason for developing OCCs to be cyber defence. but their actions in reality often indicate otherwise. For instance, although China cited cyber defence as a primary objective for the development of OCCs, her bastion of OCCs appear to be more than just a line of defence following her alleged cyber-espionage operations on Russian officials during the Russo-Ukrainian war.[43] With the increase in competition against China, the US has made a strategic shift toward a more aggressive stance of conducting offensive cyber operations in a bid to achieve tactical and strategic objectives by demonstrating her offensive capabilities in cyberspace.[44] This is evident in her increasing attacks launched on Iran, a way to boast her cyber capabilities. As per nuclear weapons, the notion of developing OCCs as an act of deterrence no longer holds true when countries with strong OCCs pose a lingering threat which cannot be paralleled. This threat extends beyond neighbouring countries to nations worldwide.

Henceforth, with many countries investing in the development of OCCs, the issue of cyber warfare becomes increasingly concerning. With the already existing geopolitical tensions, the development of

[42] "Offensive Cyber Capabilities - Infogram," Digwatch, accessed August 28, 2022, https://infogram.com/offensive-cyber-capabilities-1h7z2l87v9njx6o.

[43] Jeff Burt, "China Launches Cyber-Espionage Malware Campaign," The Register (The Register, April 27, 2022), https://www.theregister.com/2022/04/27/china-bronze-president-malware-russia/.

[44] Stratfor Worldview, "The U.S. Unleashes Its Cyberweapons | RealClearDefense," RealClearDefense, July 8, 2019, https://www.realcleardefense.com/articles/2019/07/08/the_us_unleashes_its_cyberweapons_114564-full.html.

OCCs is more likely to prompt a state-launched cyber attack as countries become increasingly armed in cyberspace, encouraging countries with developed offensive capabilities to make the first move. Clearly, the dangers of the proliferation of OCCs have to be addressed.

Rise of Self- and Semi-Regulated Markets for OCCs

The thriving cyber weapons market exacerbates the proliferation of OCCs. The trading of OCCs have skyrocketed in two main types of markets, namely self-regulated markets and semi-regulated markets. Self-regulated spaces, or black markets, operate autonomously over the dark web. In self-regulated spaces, contracts are enforced and transactions are made between OCC traders and consumers. In Operation Aurora, anonymous Chinese hackers exploited a "0day" vulnerability (a security software flaw), targeting the intellectual property and the email accounts of specific individuals in a bid to steal trade secrets from private organisations in the US.[45] Though only Google revealed the cyber attacks, many other global corporations, such as Adobe Systems and Juniper Networks, were allegedly affected by the attack. However, these corporations chose to stay silent because they wished to protect their businesses and interests in China.[46] Google ceased its operations in China and warned its users of the danger of an intrusion of their privacy. Notably, with self-regulated spaces selling increasingly sophisticated malware, they have become an increasingly lucrative market. When these malware fall into the hands of malicious actors, the cyber security of both public and private organisations, as well as the safety of personal information, will be compromised.

On the other hand, operators in semi-regulated spaces operate under the jurisdiction of the state.[47] In other words, they are legal operators acknowledged by the government. One of the key stakeholders in such spaces are actors working in Access-as-a-Service (AaaS) organisations such as Slillpp and Deer.io.[48] Such organisations sell offensive capabilities to the government for profit. In light of how governments usually establish a huge amount of budget for intelligence gathering missions, AaaS organisations are usually lucrative businesses. The money channelled into the pockets of these AaaS actors allows such services to reinvest their profits to research and development of more advanced cyber technologies.

[45] PLA Unit 61398, "Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora," Council on Foreign Relations, January 2010, https://www.cfr.org/cyber-operations/operation-aurora.

[46] "Operation Aurora - an Overview | ScienceDirect Topics," ScienceDirect, accessed August 28, 2022, https://www.sciencedirect.com/topics/computer-science/operation-aurora.

[47] Winnona DeSombre et al., "A Primer on the Proliferation of Offensive Cyber Capabilities," Atlantic Council (blog), March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

[48] Raveed Laeb, "Access-as-a-Service - Remote Access Markets in the Cybercrime Underground," Kela, May 13, 2020, https://kela.local/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/.

The Failure of Regulation of the Cyber Weapons Industry

Despite many countries having regulations for the production of cyber weapons, they are often ineffective resulting in OCCs still being prevalent among non-state actors. The failure of regulation of production of Cyber Weapons, and the fact that only a computer system is required for its production means that OCCs are extremely easy to produce.

The lack of regulation of the trading of OCC services has resulted in these services being accessible to more consumers, which is extremely undesirable for both national and global security. Black marketplaces such as Dark0de, described by Europol as "the most prolific English-speaking cybercriminal forum to date",[49] serves as a platform for the sale and trade of hacking services, botnets, malware, stolen personally identifiable information, hacked server credentials, and other illicit goods and services.[50] Although this site was reportedly taken down in 2015,[51] the site reappeared with increased security only two weeks after the announcement of the raid, employing blockchain-based authentication and operating on the Tor anonymity network.[52] It is apparent that the failure of regulation of these Black marketplaces is a reason for the proliferation of Cyber weapons.

Internationally, the lack of regulation of the cyber weapon industry due to the lack of an international standard being set, has resulted in countries amassing large numbers of OCCs. For example, China's "hacker army" personnel consists of more than 50,000 people and 250 Patriotic Hacker groups,[53] while the U.S. Army Cyber Command has 16,500 people.[54]

[49] Condé Nast, "Hacker Forum Darkode Is Back and More Secure than Ever," Wired UK, July 28, 2015, https://www.wired.co.uk/article/darkode-back-and-more-secure.

[50] Eduard Kovacs, "Hacking Forum Darkode Resurfaces | SecurityWeek.Com," SecurityWeek, July 28, 2015, https://www.securityweek.com/hacking-forum-darkode-resurfaces.

[51] "Darkode," Radiolab Podcasts | WNYC Studios, September 21, 2015, https://www.radiolab.org/episodes/darkode.

[52] Darren Pauli, "Cybercrime Forum Darkode Returns with Security, Admins Intact," The Register, July 28, 2015, https://www.theregister.com/2015/07/28/darkode_returns/.

[53] Mara Hvistendahl, "China's Hacker Army," Foreign Policy (blog), March 3, 2010, https://foreignpolicy.com/2010/03/03/chinas-hacker-army/.

[54] 'About ARCYBER | U.S. Army Cyber Command', accessed 31 October 2022, https://www.arcyber.army.mil/About/About-Army-Cyber/.

Scope of Debate

Regulation of the Cyber Weapon Industry

The lack of regulation of the production and distribution of cyber weapons can be attributed to the lack of an international agreement to start limiting the production and distribution of cyber weapons. Yet, with no such international guidelines, some countries will resort to ramping up production of cyber weapons. This could result in a cyber arms race, where countries build up an arsenal of cyber weapons, which will cause the impacts of a cyber attack to be far more devastating when it occurs.

The lack of regulation of the distribution of cyber weapons also results in cyber attacks being more prevalent. When a country's regulation of the distribution of cyber weapons in the black marketplace is insufficient, there might be more malicious cyber attacks within the country. For both the production and distribution of cyber weapons, an international standard is necessary to minimise the risk and mitigate the impacts of cyber attacks.

Countries including Russia would likely be strongly against more regulation of the cyber weapon industry as seen by their use of cyber warfare in the confrontation with Ukraine.[55] While countries such as Spain want more regulation of the cyber weapon industry as they lack cyber defences.[56] Hence, delegates will have to consider and weigh these competing ambitions and figure out a role for regulation in dealing with increased offensive cyber capabilities.

Cyber Warfare and the International Law

Vague definition of Cyber Warfare

The debate on whether cyber attacks can be considered warfare is highly contentious with experts in the field disagreeing with each other. This is due to the current vagueness regarding the definition of cyber warfare as there has yet to be an officially recognized definition of cyber warfare.[57] Therefore, to better characterise their debate, delegates may weigh potential working definitions for cyber warfare.

[55] Mary T. Tyszkiewicz and Stephen Daggett, A Defense Budget Primer (Library of Congress Washington DC Congressional Research Service, 1998), https://apps.dtic.mil/sti/citations/ADA540204.

[56] 'The Challenge of Cybersecurity in Spain: A Vulnerable Country - Telefónica', accessed 31 October 2022, https://www.telefonica.com/en/communication-room/blog/the-challenge-of-cybersecurity-in-spain-a-vulnerable-country/.

[57] Ralf Bendrath, " The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection," Critical Infrastructure Protection Initiative @ Dalhousie University, 2001, http://cip.management.dal.ca/publications/Cyberwar%20debate%20-%20perceptions%20and%20politics.pdf.

Applicability of the IHL in Cyber Warfare

Just like how conventional warfare is governed by various rules and laws such as the IHL, cyber warfare also needs to follow and respect the basic rules and principles of humanity, military necessity, distinction, proportionality and precautions. This is because cyber warfare is extremely similar to conventional warfare in terms of purpose and principles. Hence, it is very important in order to ensure the safety and dignity of people even in the troubling times of war.

As a result, debate on the application of IHL does not centre around whether the IHL should be followed, but rather how it should be applied.

A point of contention is if the personal properties of civilians should be protected during an armed conflict under Article 53 in the Fourth Geneva Convention. For now, the general consensus is that the IHL applies when cyber attacks are launched on civilian services during an armed conflict. According to the United Nations International Residual Mechanism for Criminal Tribunals, “an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups or between such groups within a State”. In the absence of armed forces, be it to target military bases or critical infrastructure of another state, it is unclear if the IHL should be applied.

Another contentious subject is whether civilian data in cyberspace should be protected the same way as civilian objects, which are all objects that are not military objectives.[58] This is because IHL only prohibits attacks on civilians and civilian objects, but does not have any clear guidelines regarding attacks on civilian data. Cyber attacks in fifth generation warfare do not only aim to injure and maim– some aim to subvert the national security of their opponents by infiltrating the sources of information of civilians. For example, in early 2022, European charity organisations involved in Ukrainian missions and helping Ukrainian refugees were targeted by hackers.[59] In spite of the absence of any physical harm caused, it is still unclear whether such war stratagems should be prohibited. Suffice to say from the example given, it is currently not clear whether the IHL applies when it comes to cyber

[58] “Customary IHL - Rule 9. Definition of Civilian Objects,” International Committee of the Red Cross, accessed October 31, 2022, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule9#:~:text=Civilian%20objects%20are%20all%20objects,and%20non%2Dinternational%20armed%20conflicts.

[59] James Pearson, “Hackers Are Targeting European Refugee Charities -Ukrainian Official,” Reuters, March 23, 2022, sec. Europe, https://www.reuters.com/world/europe/hackers-are-targeting-european-refugee-charities-ukrainian-official-2022-03-23/.

attacks and operations, and it is even more ambiguous whether cyber warfare refers to cyber attacks made during an armed conflict between countries only.

In conclusion, similar to conventional warfare that is fought physically with weapons, there are weapons, resources, and actions that should be prohibited in cyber warfare. For example, in conventional warfare, certain bioweapons are banned, and it is prohibited to attack civilians. Delegates should consider if such restrictions and rules can also be applied to cyber warfare, and if the IHL is also applicable to various situations in cyber warfare.

Self-Defence and Retaliation

The Right to Self-Defence

Unlike conventional warfare, where there is physical damage dealt to a territory of another country, what may be classified as the initiation of cyber warfare is rather difficult to define. Whether the hacking of a government database or the shutting down of a military base can be considered an attack on the country remains a point of contention, provided that a cyber attack on critical infrastructure may be just as destructive as a physical attack. Yet, with the unquantifiable nature of the magnitude of cyber attacks, it is difficult to determine when countries should be given the right to defend themselves.

Article 51 of the UN Charter gives countries the right to self-defence from armed attacks.[60] In the International Law on Self-Defence, an "armed attack" is an intentional intervention, involving the use of armed forces, in or against a state without the state's consent or subsequent acquiescence.[61] If cyber warfare is considered a type of armed attack, states would be allowed to have self-defence mechanisms under Article 51 in the UN Charter. It is, therefore, imperative for "armed attacks" to be defined, in the context of cyberspace. However, the term "cyber warfare" is ambiguous in international law. As there is no authoritative definition of "cyber warfare" in IHL,[62] different countries may interpret a cyber attack (and potentially classify it as an armed attack) differently. To wit, there is a need to standardise a set of international regulations to govern what exactly constitutes an attack which will give the victim country the right to self-defence. Countries have to collectively

[60] United Nations, "United Nations Charter (Full Text)," United Nations, August 20, 2016, https://www.un.org/en/about-us/un-charter/full-text.

[61] Wilmshurst, Elizabeth. "PRINCIPLES OF INTERNATIONAL LAW ON THE USE OF FORCE BY STATES IN SELF-DEFENCE," October 2005. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/il210211summary.pdf.

[62] "International Humanitarian Law," International Committee of the Red Cross (International Committee of the Red Cross), accessed August 2, 2022, https://www.icrc.org/en/download/file/40569/en_-_handbook_humanitarian_law_-_web.pdf.

determine the *jus ad bellum* of a cyber attack which allows the victim country to invoke its right to take action.[63]

To compound the issue further, several countries have launched cyber attacks or conducted espionage missions as a form of defence. For instance, British and American intelligence agencies declared that Operation Anarchist, a cyber spy mission to gather information from Israeli drones, was to "provide up-to-the-minute information and support to US and Allied operations in the area". To the US and UK, Israel's military actions are a potential threat to their allies in the area. This point is made even more pronounced after Israel's bombing mission in Gaza. Hence, is the launching of cyber attacks in the name of defence justified? Till this day, who and what exactly should be protected, failing which justifies a counter cyber attack, remains a largely contentious topic.

The Application of the Principle of Proportionality

Beyond merely considering the criteria to declare a just war, the degree of self-defence that can be permitted has to be determined as well. This is where the principle of proportionality, a general principle in international law, comes in.[64] In the context of the IHL, the Principle of Proportionality states that even if retaliation is allowed, it must not be excessive in relation to the expected military advantage. This concept is extremely difficult to apply in conventional warfare, and even more challenging when cyberspace is involved. The quantification of a retaliatory attack is especially difficult to determine when physical force is made use of, in response to an attack made through cyberspace. For instance, in 2019, a building housing Hamas hackers was bombed by Israel's Defence Forces.[65] The Israelis declared that the attack was made in retaliation to the cyber attacks launched by the Hamas hackers. This incident raised concerns regarding the dangerous precedence that this response sets, in using military force to address cyber threats. Is a military attack in response to a cyber attack crossing the line? Countries may claim that it is an action to defend themselves against the infringement of sovereignty. However, whether a military attack launched is commensurate with the damage dealt by the perpetrator country remains a question that has to be resolved.

Strengthening Cyber Defences

Less cyber secure countries are usually the primary targets of most cyber attacks due to their weak cyber systems and high vulnerability.

[63] Jus ad bellum is a set of criteria that need to be considered before declaring war. Essentially, it determines whether a country is justified in declaring a war.

[64] Eric Engle, "The History of the General Principle of Proportionality: An Overview," SSRN Scholarly Paper (Rochester, NY, July 7, 2009), https://papers.ssrn.com/abstract=1431179.

[65] Catalin Cimpanu, "In a First, Israel Responds to Hamas Hackers with an Air Strike," ZDNET, May 5, 2019, https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/.

There are multiple reasons for why cyber systems may be weak, such as not enforcing multi-factor authentication, outdated software, unprotected cloud services and weak password policies.[66] Besides that, local governments often operate on a shoestring budget and rarely have dedicated cybersecurity experts, choosing to just rely on their IT department instead. However, the IT department also does not have the expenditure it requires due to the government's shoestring budget. This hence weakens the government's cybersecurity considerably, leaving it vulnerable to cyber attacks.[67] Governments are also often overly reliant on third-party contractors, giving third parties with malicious intent easy access to their cyber system.[68]

To combat this, nations can strengthen their national cybersecurity through the following ways. Firstly, they can implement more preventive measures by employing anti-virus programs and detection tools that search for vulnerabilities within a system.[69] Secondly, more expenditure should also be invested into developing a nation's cyber defence. With more budget to operate on, the cybersecurity of a nation can be strengthened as more money also means more resources, such as consultations with cybersecurity experts. Lastly, nations should also tighten control on access to its cyber system. Since using the services of a third-party contractor often cannot be avoided, measures such as a zero-trust security model and conditional access policies help to prevent third parties from hacking into the national cyber system.[70] Delegates can discuss how nations are able to further strengthen their national cyber defence systems and may also wish to consider the role of international cooperation in it.

[66] Canadian Centre for Cyber Security et al., "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," Cybersecurity & Infrastructure Security Agency, May 17, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

[67] Diana Baker Freeman, "Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It," Governing , May 6, 2022, https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it.

[68] Securelink, "Why Government Institutions Are the Perfect Target for Hackers," GovTech, August 2, 2021, https://www.govtech.com/sponsored/why-government-institutions-are-the-perfect-target-for-hackers.

[69] Canadian Centre for Cyber Security et al., "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," Cybersecurity & Infrastructure Security Agency, May 17, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

[70] Canadian Centre for Cyber Security et al., "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," Cybersecurity & Infrastructure Security Agency, May 17, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

Potential Solutions

Regulations and frameworks

Delegates can consider the creation of new regulations and frameworks to regulate matters pertaining to cyber warfare. Besides that, delegates can also think about the possibility of amending and further improving on current measures. For example, the International Humanitarian Law can be amended in greater detail in order to further specify when it should be applied and make its terms less vague. In the past, protocols covering chemical weapons, landmines and laser weapons as well as many other specific areas have been added to the Geneva Conventions in 1977 and 2005,[71] showing that it is possible to amend the International Humanitarian Law as warfare in humankind evolves. These amendments can also address any loopholes that can be exploited inside the International Humanitarian Law currently.

The Establishment of Cyber Surveillance Organisations

Delegates could consider the creation of cyber surveillance organisations in close cooperation with other countries in the OSCE. Though not a method that has been previously used in Europe, it is a measure that has been taken in the past in other parts of the world. An example is the United Arab Emirates' (UAE) cyber surveillance organisation Development Research Exploitation and Analysis Department (DREAD) that was established with the help of US counterterrorism company Good Harbour Consulting.[72] With DREAD focusing on the targeting and exploitation of information derived through the use of intelligence-related cyber activities, UAE's foes were successfully hacked through this organisation.[73] Seeing as these councils have been effective solutions for other countries, delegates could consider OSCE potentially creating similar councils.

However, for this solution to be useful, delegates need to consider how to compromise between the vastly different interests of different delegations. For example, countries that are extremely vulnerable to cyber attacks will need to compromise with the countries who have strong cyber capabilities and would like to use it to their advantage. According to Comparitech's annual report on the most and least cyber secure countries around the world, four Central Asian were found to be amongst the 15 least cyber secure countries.[74] Hence, countries like these would have to compromise with more cyber

[71] "War and International Humanitarian Law - ICRC," International Committee of the Red Cross, October 29, 2010, https://www.icrc.org/en/doc/war-and-law/overview-war-and-law.htm.
[72] Christopher Bing and Joel Schectman, "Exclusive: Ex-NSA Cyberspies Reveal How They Helped Hack Foes of UAE," Reuters, January 30, 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.
[73] Ibid.
[74] Mariam Kiparoidze, "Central Asian Countries Are among the Least Cyber Secure in the World," Coda Story (blog), April 1, 2021, https://www.codastory.com/authoritarian-tech/crypromining-attack-security/.

capable countries like the United States to prevent themselves from being made targets. This could be done through the establishment of frameworks regarding the use of cyber capabilities. Besides being used for surveillance, this committee can also oversee all issues pertaining to cyber warfare as well as create and update frameworks and guidelines regarding cyber warfare (as mentioned in the above section).

Confidence-Building Measures (CBMs)

OSCE can develop a variety of confidence-building measures (CBMs). Confidence building measures refer to measures aiming to "prevent the outbreak of an [international] armed conflict by miscalculation or misperception of the risk and by the consequent inappropriate escalation of a crisis situation, by establishing practical measures and processes of [preventive] crisis management between States".[75] This is necessary and desirable to reduce the risks of tensions and conflict arising from the misuse of Information Communication Technologies (ICTs). Such CBMs include mechanisms to unite states and resolve potential cyber/ICT security cases to de-escalate mounting tensions, platforms for member states to exchange opinions and share national cyber/ICT security policies and approaches to allow states increase the transparency of national actions in the cyberspace, and concrete work items such as critical infrastructure to bolster the cybersecurity of all member nations.[76]

However, CBMs for cyberspace cannot just replicate the previously existing sets of CBMs for conventional weapons. This is because unlike traditional CBMs which were developed in a setting where states had a monopoly on the use of force and were in possession of most of the weaponry and other military means relevant to international peace and security, cyber weapons can often be found in the possession of non-state actors.[77] The main difference between controlling the use of conventional arms and cyber weapons comes down to the fact that it is very hard for States to control the quantity and production of malicious software. Hence, CBMs for cyberspace must address this different set of issues, and might be a bit harder to develop. Besides this, delegates should also take note that due to the global scope of cyberspace, any CBMs proposed cannot refer to any geographical areas.

Last but not least, it is also important to keep in mind the goals and objectives of CBMs when creating CBMs. Delegates should remember that the ultimate goal of CBMs is to strengthen international peace and security and prevent wars by reducing and eliminating the causes of mistrust, fear, misunderstanding vis-à-vis the military activities and intentions of other States.

[75] Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, 2013, https://ccdcoe.org/uploads/2018/10/CBMs.pdf.

[76] "Cyber/ICT Security," OSCE (Organisation for Security and Cooperation in Europe), accessed September 5, 2022, https://www.osce.org/cyber-ict-security.

[77] Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, 2013, https://ccdcoe.org/uploads/2018/10/CBMs.pdf.

Case Study

Operation Anarchist (USA and the Middle East)

Espionage activities in cyber warfare are prevalent. Oftentimes, powerhouses with more advanced OCCs spy on states and regions riddled with war to gather intelligence about the military capabilities of states involved, in order to better decide on the need for an intervention.[78] Such cases of meddling with foreign affairs have occurred throughout history, with one of them happening over a span of almost two decades.

Since 1998, the UK and US have been involved in an espionage activity called Operation Anarchist. It was a collaborated operation between the American National Security Agency and British Government Communications Headquarters (GCHQ). The intelligence agencies successfully broke the encryption on Israel Air Force drone transmissions and have been monitoring what the unmanned aerial vehicles (UAV) have been transmitting to their operators for several years.[79]

According to GCHQ documents, analysts first gathered encrypted video signals from a fortified site in the Troodos mountain range in Cyprus in 1998.[80] Encrypted video transmissions between drones and their bases were intercepted from Troodos and analysed using open-source software tools such as ImageMagick and AntiSky, which allowed hackers to deliberately sort through the pixels in order to decrypt them and obtain the footage.

The espionage operation also targeted drones by Syria and by Hezbollah in Lebanon. Besides that, advanced weapons systems used by Egypt, Turkey, Iran, and Hezbollah were also hacked into. UK and US intelligence also captured footage of Iranian-made drones controlled by the Syrian government. While they spied on several countries in the Middle East, the bulk of the program zoomed in on Israel and the Israeli Air Force's UAV fleet remains its primary target.[81]

The operation also tracked the movements of Israeli drones, using the special parts of transmissions when the drone would update the base on its location. The surveillance allowed the NSA and GCHQ

[78] Tara McKelvey, "US Spies on 'the Entire Globe', Experts Say," BBC News, October 25, 2013, sec. Magazine, https://www.bbc.com/news/magazine-24627187.

[79] Ronen Bergman, "US, UK Spied on Israel's Drone and Missile Programs," Ynetnews, January 31, 2016, https://www.ynetnews.com/articles/0,7340,L-4759904,00.html.

[80] Haaretz and Gili Cohen, "U.K., U.S. Spy Program Hacked Into Video Feeds on Israeli Drones, Fighter Jets," Haaretz, January 29, 2016, https://www.haaretz.com/israel-news/2016-01-29/ty-article/u-k-u-s-spy-program-hacked-into-israeli-drones-fighter-jets/0000017f-db36-df9c-a17f-ff3e41670000.

[81] Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies" (MIT Sloan School of Management, May 2017), https://cams.mit.edu/wp-content/uploads/2017-10.pdf.

to see the payloads the drones were carrying. In 2008, an internal US National Security Agency memo flaunted that the operation had been able to capture video from the cockpit of an Israeli F-16 fighter jet on a bombing mission over Gaza, displaying a target on the ground being tracked.[82]

In the same year, a GCHQ report stated that "This access [to Israel's fleet of drones] is indispensable for maintaining an understanding of Israeli military training and operations and thus an insight into possible future developments in the region."[83] The document further mentioned that "In times of crisis this access is critical and one of the only avenues to provide up-to-the-minute information and support to US and Allied operations in the area."[84]

Though the operation was meant to be confidential, it was publicly divulged in January 2016 when Edward Snowden, a US whistleblower revealed a list of documents detailing the results of the operation. It has been known as the worst intelligence breach in Israel's history.

The Strategic Affairs Minister of Israel Yuval Steinitz said Israel had always predicted that even her allies would spy on her.[85] This is a glaring example that cyber espionage is carried out even between allies, potentially eroding trust and mounting tensions between friendly nations. However, in this case, besides Israeli Prime Minister Netanyahu's claim that "in the close ties between Israel and the United States, there are things that must not be done and that are not acceptable", no concrete or reported action has been taken.[86] Although investigations were carried out, there were no results either. This leads to two possible speculations: that Israel did not retaliate against the US, aware that she had to rely on her ally for other national interests, and that it was unclear who should be held accountable and how the issue should be handled.

The lack of international effort may be subject to the murkiness of the international law governing cyber breaches and cyber warfare. On one hand, it is clear that Israel was engaging in suspicious military activities, according to footage captured by US and UK intelligence. The Israeli drones collected intelligence on the West Bank, the Gaza Strip, and across the Middle East, and analysts have

[82] "US and UK 'Hacked into Israeli Drones and Planes,'" BBC News, January 29, 2016, sec. Middle East, https://www.bbc.com/news/world-middle-east-35440523.

[83] Cora Currier and Henrik Moltke, "Israeli Drone Feeds Hacked By British and American Intelligence," The Intercept, January 28, 2016, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/.

[84] Ibid.

[85] "Netanyahu Says Any U.S. Spying on Israel Unacceptable," Reuters, December 23, 2013, sec. Editor's Picks, https://www.reuters.com/article/us-israel-usa-spying-idUSBRE9BM0IG20131223.

[86] "Netanyahu Says Any U.S. Spying on Israel Unacceptable," Reuters, December 23, 2013, sec. Editor's Picks, https://www.reuters.com/article/us-israel-usa-spying-idUSBRE9BM0IG20131223.

suspected a potential Israeli strike on Iran.[87] But on the other hand, the US and UK were clearly infringing on Israel's sovereignty by hacking into their drone systems. This places the two nations in a moral equilibrium of sorts, which may be the reason for the lack of action taken. But on top of that, there are also several complications in the realm of cyber warfare and international law which may have given rise to this stalemate. The US merely captured footage of drones but did not launch a physical attack on Israel. So does this count as an armed attack and does it justify retaliation from Israel? Besides that, in a report, the US claimed that she is "support[ing] US and allies operations in the area".[88] Could this be considered an act of self-defence for the US and her allies that may have been affected by Israel's military activities, considering that an Israeli attack is merely presumptive? On the side note, the US and UK did not inflict any sort of physical damage on Israel. Hence, if Israel were to retaliate against the cyber infiltration of the two countries, what should be the magnitude of their counterattack?

This noteworthy case study demonstrates the importance of a more detailed and transparent international law governing cyber warfare, as well as the actions that should be taken against perpetrator countries to prevent such cyber breaches from happening again. If left unaddressed, state-launched cyber attacks will only continue to proliferate in the future, exacerbating geopolitical tensions all around the world.

[87] Ronen Bergman, "US, UK Spied on Israel's Drone and Missile Programs," Ynetnews, January 31, 2016, https://www.ynetnews.com/articles/0,7340,L-4759904,00.html.

[88] Ronen Bergman, "US, UK Spied on Israel's Drone and Missile Programs," Ynetnews, January 31, 2016, https://www.ynetnews.com/articles/0,7340,L-4759904,00.html.

Key Stakeholders

Countries vulnerable to potential cyber attacks

Countries that stand a lot to lose during cyber attacks are countries that rely heavily on key infrastructure. Examples of such countries are Tajikistan, Uzbekistan, Kazakhstan and Kyrgyzstan, which have the highest percentage of attacks from cryptominers according to an annual report by Comparitech.[89] Such infrastructure is usually targeted during cyber attacks, making these countries especially vulnerable to potential cyber attacks. Other than countries that are reliant on key infrastructure, developing countries are also especially vulnerable to cyber attacks as they afford the relevant surveillance due to limited financial resources. As a result, developing countries have a very weak surveillance capacity and a decreased ability to respond to threats in time. Hence, developing countries are more vulnerable to cyber attacks.

As countries that are vulnerable to cyber attacks, these countries are likely to be against the use of offensive cyber capabilities of any kind. Besides being against the use of cyber offence, these countries will also likely advocate for the strengthening of their national cybersecurity systems, especially through collaboration with other countries. This is because collaboration means faster strengthening of the country's national cybersecurity systems and a pool of shared resources. Additionally, working with other countries in a collaborative manner also means that the countries' systems are influenced by each other, and that a cyber attack on one country could necessitate the response of another country. This is good as with the mutual support of the countries involved, these countries' cybersecurity is likely to be strengthened, preventing such cyber attacks in the future.

Countries and non-state actors which mass produce and sell offensive cyber capabilities

Countries and non-state actors which mass produce and sell offensive cyber capabilities are likely to be against any countermeasures restricting the trade of offensive cyber capabilities as this can bring significant losses to them. At the same time, they will also try to deflect any blame for cyber attacks that might originate from their sale of offensive cyber capabilities as this could be disadvantageous to their trade. Hence, they are likely to propose compromises or exploit loopholes such that they can continue with their sale of offensive cyber capabilities, even if it must be done so in secret.

[89] Mariam Kiparoidze, "Central Asian Countries Are among the Least Cyber Secure in the World," Coda Story (blog), April 1, 2021, https://www.codastory.com/authoritarian-tech/crypromining-attack-security/.

Countries with strong offensive and defensive capabilities

Countries with both strong offensive and defensive cyber capabilities can contribute greatly to preventive measures against cyber attacks by using their strong digital infrastructure as an example for countries with weaker offensive and defensive capabilities. By sharing information and resources, these countries can help to strengthen the cybersecurity of the countries in OSCE as a whole. Examples of countries that have strong defensive and offensive cyber capabilities in the OSCE are Russia and the United States.[90]

However, not all countries with strong offensive and defensive cyber capabilities will be amenable to sharing such information as having a secure cyber defence gives the country an advantage over all the other countries in OSCE. Some countries might even be more open to launching cyber attacks against other countries and starting cyber warfares as they are confident of their own country's cyber capabilities to remain secure from cyber attacks. Hence, these countries are likely to be against measures that restrict the use of cyber capabilities as this gives an advantage to them as a country with stronger cyber capabilities.

[90] Keith Breene, "Who Are the Cyberwar Superpowers?," World Economic Forum, May 4, 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

Questions A Resolution Must Answer (QARMA)

1. How should cyber warfare be defined and how will OSCE work with this definition in subsequent debates?
2. How should OSCE manage cyber warfare going forward and minimise the harm created by cyberwarfare?
3. How will OSCE differentiate developments in general cybertechnology from cyber weapons that could cause cyber warfare?
4. Should the cyber weapon industry be regulated? If so, how?
5. How will the principles and rules of war be applied in the context of cyber warfare?
    a. How will the International Humanitarian Law be applied in the context of cyber warfare?
    b. How will the Principle of Proportionality be applied in the context of cyber warfare?

Conclusion

With the world's increasing reliance on technology in today's age, cyber warfare is a threat that will collectively affect all of us unless greater action is taken to regulate it. In recent years, many of the interstate cyber attacks launched could actually inflict physical damage, indicating that cyberspace should be taken more seriously as a domain of war, just like the land, sky and sea.

Without the relevant regulations and amendments to current legislation, it will be hard for countries to defend their land and citizens against the damage that a cyber attack can cause. To make things worse, countries will basically be fighting an anonymous threat that they cannot even see, hiding within devices that they use almost daily. As such, besides taking cyber warfare more seriously as a threat, it is also important to regulate cyber warfare more strictly to protect civilians. Besides this, it is also crucial to strengthen one's own country's defence against cyber attacks by investing more into the area, updating current operations systems to keep up with the ever-evolving threat of cyber warfare.

Seeing how the topic is complex in nature, while bearing in mind the never-ending evolution of technology, cyber warfare will continue to remain a contentious issue in the years to come. To combat the threat of cyber warfare, delegates should aim to address current flaws in existing policies and work together to come up with new solutions while keeping in mind their country's various interests and agendas.

Bibliography

“Armed Conflict » ICTR/ICTY/IRMCT Case Law Database,” United Nations International Residual Mechanism for Criminal Tribunals, accessed September 21, 2022, https://cld.irmct.org/notions/show/93/armed-conflict.

“Check Point Research: Cyber Attacks Increased 50% Year over Year,” Check Point Software, January 10, 2022, https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/.

“Critical Infrastructure Sectors | CISA,” Cybersecurity & Infrastructure Security Agency (Cybersecurity & Infrastructure Security Agency, October 21, 2020), https://www.cisa.gov/critical-infrastructure-sectors.

“Customary IHL - Rule 9. Definition of Civilian Objects,” International Committee of the Red Cross, accessed October 31, 2022, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule9#:~:text=Civilian%20objects%20are%20all%20objects,and%20non%2Dinternational%20armed%20conflicts.

“Cyber Warfare: Does International Humanitarian Law Apply?,” February 15, 2021, https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.

“Cyber/ICT Security,” OSCE (Organisation for Security and Cooperation in Europe), accessed September 5, 2022, https://www.osce.org/cyber-ict-security.

“Darkode,” Radiolab Podcasts | WNYC Studios, September 21, 2015, https://www.radiolab.org/episodes/darkode.

“History,” Organisation for Security and Co-operation in Europe, accessed July 31, 2022, https://www.osce.org/who/87.

“Information and Communication Technologies (ICT) | Unesco IIEP Learning Portal,” UNESCO International Institute for Educational Planning (UNESCO International Institute for Educational Planning), accessed August 1, 2022, https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict.

“International Humanitarian Law,” International Committee of the Red Cross (International Committee of the Red Cross), accessed August 1, 2022, https://www.icrc.org/en/download/file/40569/en_-_handbook_humanitarian_law_-_web.pdf.

“Iranian Offensive Cyber Attack Capabilities” (Congressional Research Service, January 13, 2020), https://sgp.fas.org/crs/mideast/IF11406.pdf.

"Malware, Trojan, and Spyware – Information Security," California State University, Chico (California State University, Chico), accessed September 15, 2022, https://www.csuchico.edu/isec/stories/malware-trojans-spyware.shtml.

"Netanyahu Says Any U.S. Spying on Israel Unacceptable," Reuters, December 23, 2013, sec. Editor's Picks, https://www.reuters.com/article/us-israel-usa-spying-idUSBRE9BM0IG20131223.

"Offensive Cyber Capabilities - Infogram," Digwatch, accessed August 28, 2022, https://infogram.com/offensive-cyber-capabilities-1h7z2l87v9njx6o.

"Operation Aurora - an Overview | ScienceDirect Topics," ScienceDirect, accessed August 28, 2022, https://www.sciencedirect.com/topics/computer-science/operation-aurora.

"Stuxnet - The First Cyber Weapon," Gemserv (Gemserv, December 31, 2019), https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/.

"Treaties, States Parties, and Commentaries - Geneva Convention (IV) on Civilians, 1949 - 53 - Prohibited Destruction," International Committee of the Red Cross, August 12, 1949, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/380-600060?OpenDocument.

"UN Resolutions," ITU, accessed October 31, 2022, https://www.itu.int:443/en/action/cybersecurity/Pages/un-resolutions.aspx.

"US and UK 'Hacked into Israeli Drones and Planes,'" BBC News, January 29, 2016, sec. Middle East, https://www.bbc.com/news/world-middle-east-3

"War and International Humanitarian Law - ICRC," International Committee of the Red Cross, October 29, 2010, https://www.icrc.org/en/doc/war-and-law/overview-war-and-law.htm.

Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," Time (Time, April 18, 2019), https://time.com/5565991/russia-influence-2016-election/.

Adam Segal, "Cyber Conflict After Stuxnet," Council on Foreign Relations (blog), June 27, 2016, https://www.cfr.org/blog/cyber-conflict-after-stuxnet.

Andrea Shalal-Esa, "Iran Strengthened Cyber Capabilities after Stuxnet: U.S. General," Reuters, January 18, 2013, sec. Technology News, https://www.reuters.com/article/us-iran-usa-cyber-idUSBRE90G1C420130118.

Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Stanford (Stanford, 2011), http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.

Brijesh Singh, "India's Cybersecurity and Its Impact on the Economy," Gateway House (blog), August 4, 2022, https://www.gatewayhouse.in/indias-cybersecurity-and-its-impact-on-the-economy/.

Canadian Centre for Cyber Security, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, Government Communications Security Bureau, National Cyber

Security Centre, and National Security Agency. “Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA.” Cybersecurity & Infrastructure Security Agency, May 17, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

Catalin Cimpanu, “In a First, Israel Responds to Hamas Hackers with an Air Strike,” ZDNET, May 5, 2019, https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/.

Christopher Bing and Joel Schectman, “Exclusive: Ex-NSA Cyberspies Reveal How They Helped Hack Foes of UAE,” Reuters, January 30, 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

Chuck Brooks, “Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know,” Forbes, June 3, 2022, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/.

Condé Nast, “Hacker Forum Darkode Is Back and More Secure than Ever,” Wired UK, July 28, 2015, https://www.wired.co.uk/article/darkode-back-and-more-secure.

Cora Currier and Henrik Moltke, “Israeli Drone Feeds Hacked By British and American Intelligence,” The Intercept, January 28, 2016, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/.

Darren Pauli, “Cybercrime Forum Darkode Returns with Security, Admins Intact,” The Register, July 28, 2015, https://www.theregister.com/2015/07/28/darkode_returns/.

David E. Sanger, Nicole Perlroth, and Eric Schmitt, “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit,” The New York Times, December 15, 2020, sec. U.S., https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Diana Baker Freeman, “Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It,” Governing , May 6, 2022, https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it.

Eduard Kovacs, “Hacking Forum Darkode Resurfaces | SecurityWeek.Com,” SecurityWeek, July 28, 2015, https://www.securityweek.com/hacking-forum-darkode-resurfaces.

Eric Engle, “The History of the General Principle of Proportionality: An Overview,” SSRN Scholarly Paper (Rochester, NY, July 7, 2009), https://papers.ssrn.com/abstract=1431179.

Florian Egloff and James Shires, “Offensive Cyber Capabilities and State Violence: Three Logics of Integration,” Oxford Academic (Oxford Academic, October 26, 2021), https://academic.oup.com/jogss/article/7/1/ogab028/6412386.

Florian Egloff and James Shires, “Offensive Cyber Capabilities and State Violence: Three Logics of Integration,” Oxford Academic (Oxford Academic, October 26, 2021), https://academic.oup.com/jogss/article/7/1/ogab028/6412386.

Haaretz and Gili Cohen, “U.K., U.S. Spy Program Hacked Into Video Feeds on Israeli Drones, Fighter Jets,” Haaretz, January 29, 2016, https://www.haaretz.com/israel-news/2016-01-29/ty-article/u-k-u-s-spy-program-hacked-into-israeli-drones-fighter-jets/0000017f-db36-df9c-a17f-ff3e41670000.

Haaretz, “U.K.-U.S. Spy Operations Also Reportedly Targeted Israeli Missile Project,” Haaretz, January 31, 2016, sec. Middle East News, https://www.haaretz.com/middle-east-news/2016-01-31/ty-article/u-k-u-s-spy-operations-also-reportedly-targeted-israeli-missile-project/0000017f-da75-d42c-afff-dff7df430000.

Heather Landi, “Relentless Cyberattacks Are Putting Financial Pressure on Hospitals: Fitch Ratings,” Fierce Healthcare, July 26, 2021, https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings.

Irene Tham et al., “Singapore’s Worst Cyber Attack: How It Unfolded,” The Straits Times (The Straits Times, July 20, 2018), https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

Jakub Przetacznik, “Russia’s War on Ukraine: Timeline of Cyber-Attacks | Think Tank | European Parliament,” European Parliament, June 21, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549.

James Andrew Lewis, “Cyber War and Ukraine,” Center for Strategic & International Studies (Center for Strategic & International Studies, June 16, 2022), https://www.csis.org/analysis/cyber-war-and-ukraine.

James Pearson, “Hackers Are Targeting European Refugee Charities -Ukrainian Official,” Reuters, March 23, 2022, sec. Europe, https://www.reuters.com/world/europe/hackers-are-targeting-european-refugee-charities-ukrainian-official-2022-03-23/.

Jeff Burt, “China Launches Cyber-Espionage Malware Campaign,” The Register (The Register, April 27, 2022), https://www.theregister.com/2022/04/27/china-bronze-president-malware-russia/.

Joel Schectman et al., “Exclusive: Microsoft Believes Russians That Hacked Clinton Targeted Biden Campaign Firm - Sources,” Reuters, September 10, 2020, sec. Banks, https://www.reuters.com/article/us-usa-election-cyber-biden-exclusive-idUSKBN2610I4.

Josh Gold, “Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?,” Council on Foreign Relations, March 18, 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

Jowi Morales, “Why Hackers Target Critical Infrastructure and Why It’s Difficult to Upgrade Cybersecurity,” MUO, May 7, 2022, https://www.makeuseof.com/why-hackers-target-critical-infrastructure/.

Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, 2013, https://ccdcoe.org/uploads/2018/10/CBMs.pdf.

Keith Breene, “Who Are the Cyberwar Superpowers?,” World Economic Forum, May 4, 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

Mara Hvistendahl, “China’s Hacker Army,” Foreign Policy (blog), March 3, 2010, https://foreignpolicy.com/2010/03/03/chinas-hacker-army/.

Mariam Kiparoidze, “Central Asian Countries Are among the Least Cyber Secure in the World,” Coda Story (blog), April 1, 2021, https://www.codastory.com/authoritarian-tech/crypromining-attack-security/.

Mary T. Tyszkiewicz and Stephen Daggett, A Defense Budget Primer (Library of Congress Washington DC Congressional Research Service, 1998), https://apps.dtic.mil/sti/citations/ADA540204.

Mohan B. Gazula, “Cyber Warfare Conflict Analysis and Case Studies” (MIT Sloan School of Management, May 2017), https://cams.mit.edu/wp-content/uploads/2017-10.pdf.

Nicole Sganga, Catherine Herridge, and Musadiq Bidar, “Foreign Hacking Group Targets Hospitals, Clinics with Ransomware Attacks, Says New Report,” CBS News (CBS News, October 7, 2021), https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups/.

PLA Unit 61398, “Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora,” Council on Foreign Relations, January 2010, https://www.cfr.org/cyber-operations/operation-aurora.

Ralf Bendrath, “ The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection,” Critical Infrastructure Protection Initiative @ Dalhousie University, 2001, http://cip.management.dal.ca/publications/Cyberwar%20debate%20-%20perceptions%20and%20politics.pdf.

Raveed Laeb, "Access-as-a-Service - Remote Access Markets in the Cybercrime Underground," Kela, May 13, 2020, https://kela.local/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/.

Reuters Staff, "Anthem to Pay Nearly $40 Million to Settle Data Breach Probe by U.S. States," Reuters, September 30, 2020, sec. U.S. Legal News, https://www.reuters.com/article/us-anthem-cyber-idUSKBN26L2PW.

Richard Speed, 'Albanian Government Websites Go Dark after Cyberattack', accessed 31 October 2022, https://www.theregister.com/2022/07/18/albania_down/.

Ronen Bergman, "US, UK Spied on Israel's Drone and Missile Programs," Ynetnews, January 31, 2016, https://www.ynetnews.com/articles/0,7340,L-4759904,00.html.

Ryan Gallagher and Kitty Donaldson, "Bloomberg - Are You a Robot?," December 14, 2020, https://www.bloomberg.com/news/articles/2020-12-14/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack.

Securelink, "Why Government Institutions Are the Perfect Target for Hackers," GovTech, August 2, 2021, https://www.govtech.com/sponsored/why-government-institutions-are-the-perfect-target-for-hackers.

Stratfor Worldview, "The U.S. Unleashes Its Cyberweapons | RealClearDefense," RealClearDefense, July 8, 2019, https://www.realcleardefense.com/articles/2019/07/08/the_us_unleashes_its_cyberweapons_114564-full.html.

Tara McKelvey, "US Spies on 'the Entire Globe', Experts Say," BBC News, October 25, 2013, sec. Magazine, https://www.bbc.com/news/magazine-24627187.

United Nations, "United Nations Charter (Full Text)," United Nations, August 20, 2016, https://www.un.org/en/about-us/un-charter/full-text.

What Is a Cyber Attack?," Check Point Software, accessed August 1, 2022, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/.

Wilmshurst, Elizabeth. "PRINCIPLES OF INTERNATIONAL LAW ON THE USE OF FORCE BY STATES IN SELF-DEFENCE," October 2005. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/il210211summary.pdf.

Winnona DeSombre et al., "A Primer on the Proliferation of Offensive Cyber Capabilities," Atlantic Council (blog), March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.