LmunA 2022

Research report

Forum:	Disarmament and International Security Committee
Issue:	Reviewing cyber-hacking as a breach of international security
Student Officer:	Ana Sofia White
Position:	Deputy Chair

LMUNA
Lorentz Lyceum
Model United Nations
Arnhem

Table of Contents

Introduction

While bringing forth groundbreaking leaps in our existence as a civilization, the recent surge in technological advancements during the past few decades has also been a point of vulnerability in our societies. As we become increasingly intertwined with technology in our everyday lives, we run the risk of its capability of being a threat to our fragile, interconnected world. This is why now more than ever we must look to the LmunA 2022 theme of Emerging Technologies in Shaping Modern Society. We must find ways to limit a potentially detrimental fate with technology, while continuing to use our relationship with it for good.

Moving forward we must note that cyber-hacking and cyber-warfare is susceptible to further deterioration of the peaceful conversations facilitated in the UN among member states, and place focus on alternatives to protect the well being of individuals, firms and states. As delegates in the UN, tasked with the responsibility of peacekeeping, and especially delegates in GA1 placing an emphasis on international security and disarmament, delegates should explore the issues surrounding these delicate topics and propose concrete actions that can be taken to mitigate these risks. This report aims to provide delegates with the necessary knowledge to achieve this goal.

Definitions of key terms

Cyber-hacking

Any form of an attempt carried out by an individual or organisation to weaken or destroy computer information systems, computer networks and/or personal computers through means of stealing, altering or damaging a source.

Security

The state of being free from danger or harm's way.

Cyber security

The protection from computerised information, networks and computer systems from being stolen, harmful use, and/or used without permission.

Cyber-warfare

Digital infrastructure used by computers and networks connecting them, usually by the military network of a country, to gain advantage over an opponent. This can be through tampering with, altering or preventing the use of the opposing countries networks.

Computer networks

Varying in scope, they connect computers over a certain physical area to exchange information, resources or services.

Espionage

The state of being in possession of confidential military, political, commercial or other information on a country or group through ways of spying or illegal monitoring devices, generally known as being illegal.

General overview

Cyber hacking is a form of warfare. In general, states and international organisations deploy cyber warfare in an attempt to undermine other countries' computers and information networks which include: power grids, internet networks, nuclear weapon programs, private companies and democratic processes. Similarly, cyber attacks can be targeted at specific geographic regions or companies. Conversely, despite the precision, attacks can be difficult to detect. While different forms of cyber warfare have been occurring for years, the most destructive cyber attacks have been taking place in the last decade and a half.

Identifying cyber-attacks

Cyber warfare has many challenges that can make it difficult for countries and international organisations to control and defend against. Cyber attacks often take place in a concealed manner and are designed to not be recognizable. Civilians and private sector companies that often want to keep their identities hidden may also launch their own cyber attacks outside of direct government control. Some cyber attacks could also be deployed in an effort to distract the opposition for more complex operations. Furthermore, since cyber attacks are often not directly linked to or integrated with traditional armed conflict, it is not always apparent how they benefit military victories. In light of these factors, it can be difficult for countries to determine the intended targets, source, or political, economic and/or security objectives of the attacks.

The human rights dimension of cyber warfare.

Cyber warfare has a human rights dimension. A form of cyber warfare involves disrupting the internet and hacking private accounts. As noted by Human Rights Watch, internet shutdowns prevent individuals from being able to find objective information, exchange dissenting views, work, continue their education, or access government services. Government hacking of personal communications can lead to violations of privacy and other human rights abuses such as wrongful imprisonments and executions.

A potentially safer form of conflict

Some have argued that despite the potential risks, cyber warfare could make the world safer. The Washington Post reports that cyber warfare could offer a means for states to achieve their political objectives without engaging in physical, armed conflict. For example, in 2007, Israel bombed a suspected nuclear weapons facility in Syria. While the attack was successful, approximately ten scientists from North Korea may have been killed and many countries harshly criticised Israel. However, between 2007 and 2010, the US and Israel deployed a computer virus in Iran to much greater effect. The virus is believed to have destroyed nearly a fifth of Iran's operating nuclear centrifuges and set its nuclear weapons program back by two years with no lives lost.

Major parties involved

Russia

Russia has long been accused of cyber attacks as a form of espionage in the U.S, Ukraine and North Korea to name a few countries. Currently, Russia is releasing several forms of cyber attacks targeting both private and public sectors in parallel with its invasion of The Ukraine. In instances where the country has been accused of harmful forms of cyber-hacking, it always denied playing a role.

China

Having a strong military presence globally, China's stance is both similar to and in line with Russia. Like its counterpart it has been accused during several instances of harmful acts of cyber-hacking and espionage, such as in the U.S, UK and Taiwan.. An example of this can be seen when Taiwan accused China of releasing a cyber campaign against many important businesses as a disapproval of the reelection of Taiwan's president. Equally, when provided with evidence of involvement in national cyberhacking, China only denies its role.

Israel

After mounting evidence in December of 2021, that technology developed by Israeli firms such as NSO group was used by foreign governments in espionage on civilians, the country has decided to strengthen its management of cyber security exports. The company has also received lawsuits from other social-media companies based in the U.S. such as Apple and Facebook for its responsibility in the companies being hacked by NSO's spyware, Pegasus. Should countries want to buy Isreali technology, they must sign a declaration that it will be use "for the investigation and prevention of terrorist acts and serious crimes only"

USA

As a long standing global military power, the US has implemented different forms of protection against cyber-hacking. In its executive order in May of 2021, on improving the nation's cybersecurity the USA states that they need to "make bold changes and significant investments in order to defend the vital institutions that underpin American way of life". In other words, the country is dedicating plentiful resources to adapt to the changing climate of cyber-hacking, in its movement to "partner with the private sector". Also, to protect its own national security, especially under the Biden administration the U.S. has placed a ban on all hacking tools to Russia, China and other countries without a licence from the department's Bureau of Industry and Security (BIS).

The Human Rights Watch

As a pertinent NGO, their aim is to advocate for sufficient legislative work to enforce and respect human rights in the operations of the UN. HRW believes that cyberattacks can translate into human rights abuses. This is because fundamental rights are at stake when governments engage in cyberattacks, like when Russia shut down the internet, as it did in Crimea in 2016 or when a government hacks into a dissident or journalist's phone, as Saudi Arabia and UAE have repeatedly done.

Internet shutdowns deny people access to critical information, the ability to express themselves, work, learn, and access social services. Government hacking infringes on privacy and can lead to other rights violations, in particular for human rights activists and journalists.

Timeline of Key Events

1969 The first early computer network, called ARPANET, was established by the Pentagon's Advanced Research Projects Agency.

1971 For the first time a program is designed to move from one computer to another on its own, being the first experimental computer worm called "Creeper".

1973 The first cybersecurity program, called "Reaper" is designed to eliminate the 1971's Worm "Creeper"

1983 Transmission control protocol/ internet protocol(TCP/IP) became the global standard for network communications, allowing networks all over the world to communicate with each other, giving rise to the internet.

1988 A university student created and released the first internet worm infecting and crashing 10% of the 60,00 computers connected to the internet.

1990 The Computer Misuse Act is passed in the UK establishing any attempts to access an external computer network that are not permitted by the network owner(s) as illegal.

1991 The European Institute for Computer Anti-Virus Research (EICAR) is established to carry out antivirus research and development of antivirus software.

2000 A worm called "ILOVEYOU" spread via email so quickly that the Pentagon and CIA shut down.

2010 A hardware virus created in a collaboration between the U.S. National Security Agency, the CIA, and Israeli intelligence.called "Stuxnet" disrupted Iran's nuclear program being one of the first instances of cyberattacks used in espionage.

2013-2014 Yahoo suffers the largest data breach in history, which resulted in a theft of 3 billion users personal data, a 35 million dollar fine and 40 Lawsuits.

2016 A piece of malware given the name Indestroyer is the first ever to hack a power grid in Kyiv, The Ukraine affecting what is estimated to be more than 80,000 customers in 8 different regions of the city. State-sponsored Russian hackers have been accused of the orchestrating event.

2018 The EU enforces general data protection regulation (GDPR).

2019 The UN Office of Counter-Terrorism implemented Phase I of the Cybersecurity Programme for South East Asia and Bangladesh, delivering an awareness raising workshop for the 11 beneficiary Member States. A pilot in-depth training workshop was also organised for Thailand, Brunei, Philippines, Bangladesh and Lao PDR.

Also, a type of cyber attack called Distributed Denial of Service (DDoS) flooded New Zealand's stock market with internet traffic, forcing it temporarily shut down.

2020 The UN Office of Counter-Terrorism will implement Cybersecurity Phase I for East Africa, Horn of Africa and the Sahel.

2022 Russia releases a multitude of cyber attacks alongside its military in its invasion of The Ukraine.

Previous attempts to solve the issue

One example of an attempt to mitigate the risks of cyber-hacking was during the sixth review of the Global Counter-Terrorism Strategy by the UNCCT. The review provided a mandate on cyber-hacking while placing an emphasis on the role of terrorist groups in perpetuating the threat of cyber attacks among member states. The critique of the resolutions passed during the review, by observing third parties, was the negative impact of a greater dependence on military intervention in the counterterrorism strategy. Another critique was the lack of a safe environment provided by the strategy of the resolutions for humanitarian workers, especially including women, to carry out their initiatives.

In December of 2019 a resolution was passed by the General Assembly on “countering the use of information and communications technologies for criminal purposes”, introducing an Ad Hoc committee. Recently this year, after three years in the making, the first two meetings of a newly created international treaty on cybercrime, formulated following the passed resolution, took place in March and late May to early June. Although the committee is said to take three more years in its endeavours, based on what has already been discussed, the main critique of the it is that member states cannot come to an agreement on what a cyber crime does and does not consist of and also the extent of the role the committee will play in discussion surround cyber warfare.

Additionally, the UN Office of Counter-Terrorism (UNOCT) has a cybersecurity program designed to support member stated and organizations in preventing cyber-attacks against critical infrastructure. Several initiatives have been launched in the field of new technologies, including a project on the use of social media to gather open source information and digital evidence to counter terrorism and violent extremism while respecting human rights.

Possible solutions

In order to ensure that cyber warfare does not lead to open armed conflict between states with lethal consequences, treaties and unwritten customary laws are required to modulate its use, such as a digital Geneva Convention that requires counties to apply their cyber weapons within set limits and prohibit the destruction of civilian infrastructure. Furthermore to better disincentive acts of harmful cyber-hacking a clearer definition of what constitutes an offensive attack is needed to appropriately penalise member states that override the agreed definition.

As this issue aims to solve the threat of cyber hacking as a breach of international security, more international cybersecurity cooperation is needed among member states. This can take place through means of sharing data protection strategies, research in the fields of antiviruses

and malware, to name a few, and general experience. The intention behind collective cooperation will also be to strengthen trust and public and private partnerships among member states. This could be through means such as training, using communications or emergency warning networks among others, ultimately in hopes of reducing countries' dependence on the offensive benefit of cyber-hacking.

To better mitigate the current situation in regions that have suffered from the terrorist attacks and damage to infrastructure more advocacy for a safer environment peacekeeping organisations. Their role in serving as objective parties to enforce the agreed upon limits to attacks and providing humanitarian support, must also be respected and protected to sufficiently manage any consequences of cyber attacks.

Further reading

1. "Letter Dated 15 December 2015 from the Chair of the Security Council Committee Established pursuant to Resolution 1373 (2001) Concerning Counter-Terrorism Addressed to the President of the Security Council." UN.org, 2015, documents-dds-ny.un.org/doc/UNDOC/GEN/N15/448/85/PDF/N1544885.pdf?OpenElement. Accessed 14 July 2022.

2. "Resolution 2341 (2017)." UN.org, 2017, documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/57/PDF/N1703857.pdf?OpenElement. Accessed 2022.

3. "Resolution 2370 (2017)." UN.org, 2017, documents-dds-ny.un.org/doc/UNDOC/GEN/N17/241/71/PDF/N1724171.pdf?OpenElement. Accessed 2022.

4. "Resolution Adopted by the General Assembly on 26 June 2018." UN.org, 2018, documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/80/PDF/N1819880.pdf?OpenElement. Accessed 2022.

Bibliography

Works Cited

Baghdasaryan, Meri. “UN Committee to Begin Negotiating New Cybercrime Treaty amid Disagreement among States over Its Scope.” *Electronic Frontier Foundation*, 15 Feb. 2022, www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among. Accessed 14 July 2022.

“Convention on Cybercrime.” *Wikipedia*, Wikimedia Foundation, 13 July 2022, en.wikipedia.org/wiki/Convention_on_Cybercrime#:~:text=The%20Convention%20on%20Cybercrime%2C%20also,and%20increasing%20cooperation%20among%20nations. Accessed 14 July 2022.

“Cybersecurity | Office of Counter-Terrorism.” *Un.org*, 2018, www.un.org/counterterrorism/cct/programme-projects/cybersecurity. Accessed 14 July 2022.

Federman, Josef. “Fearing Misuse, Israel Tightens Supervision of Cyber Exports.” *AP NEWS*, Associated Press, 6 Dec. 2021, apnews.com/article/technology-business-middle-east-israel-global-trade-487ba2e28705e14d94a6f959cdaedea2. Accessed 14 July 2022.

“Global Group of NGOs Deplore Lack of Attention to Human Rights in Latest Review of UN’s Global Counterterrorism Strategy by UN Member States.” *International Federation for Human Rights*, 2018, www.fidh.org/en/global-group-of-ngos-deplore-lack-of-attention-to-human-rights-in. Accessed 14 July 2022.

Klevering, Griffin. “A Brief Look at Chinese Cyberwarfare | Small Wars Journal.” *Smallwarsjournal.com*, 2022, smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare. Accessed 14 July 2022.

Knell, Noelle. “Top 10 Countries Where Cyber Attacks Originate.” *GovTech*, GovTech, 23 Apr. 2013, www.govtech.com/security/hacking-top-ten.html. Accessed 14 July 2022.

Page, Carly. “US Government Bans Sale of Hacking Tools to China and Russia.” *TechCrunch*, TechCrunch, 20 Oct. 2021, techcrunch.com/2021/10/20/commerce-ban-hacking-tools-china-russia/?guccounter=1&guce_referrer=aHR0cHM6Ly9wb3J0c3dpZ2dlci5uZXQv&guce_referrer_sig=AQAAAAkYpEenOx6w6ZtL1ME4hVAQgmaI_hUU3pBubFPM_u-R-e-TqL7GvaqpUS8gCf7mPK8gkDoeu93mJZpXTOpPT_aTwhRBE9rg-qKdzGBpvXklOn_b64U5y611OHI_uABNoZqo5ScBP6bJxOVwIoM6PAh12-w6nQ4Hc45qe2VN6Cfn. Accessed 14 July 2022.

“The History of Cybersecurity: CompTIA’s Future of Tech.” *CompTIA’s Future of Tech*, 2012, www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/. Accessed 14 July 2022.

The White House. “Executive Order on Improving the Nation’s Cybersecurity | the White House.” *The White House*, The White House, 12 May 2021, www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Accessed 14 July 2022.

Townsened, Caleb. “Cyber Security Summit – Philadelphia.” *United States Cybersecurity Magazine*, 18 Jan. 2019, www.uscybersecurity.net/history/. Accessed 14 July 2022.

"Trellix." *Trellix.com*, 2022, www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html#:~:text=Stuxnet%20is%20a%20computer%20worm,used%20to%20automate%20machine%20processes. Accessed 14 July 2022.

Zetter, Kim. "Everything We Know about Ukraine's Power Plant Hack." *Wired*, WIRED, 20 Jan. 2016, www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. Accessed 14 July 2022.