Forum: Security Council

Issue: Addressing the global threat of cyber warfare

Student Officer: Jack Ma

Position: President

Introduction

Since the modern internet's inception on January 1, 1983, malware has been a part of the collective human consciousness. However, what happens when one takes a run-of-the-mill virus and upscales it to attack an entire country? This is the issue of cyber warfare - a cyberattack or series of cyberattacks directed not at an individual but at a country to damage government or civilian infrastructure and cause damage to the state and potential deaths ("What Is Cyber Warfare | Types, Examples & Mitigation | Imperva").

Cyberattacks can be especially difficult to mitigate since the Internet landscape is constantly changing due to the development of new technologies. New advancements in software provide new ways for malware to spread as well. Since technology is developing at "warp speed" (Guterres), the rate of cyberattacks is increasing as well, especially for countries involved in conflicts and underdeveloped regions (e.g., Ukraine, Kenya, etc.)

Methods to combat cyber warfare have been proposed, such as in the Cooperative Cyber Defense Center of Excellence's (CCDCoE) Tallinn Manual. However, since attacks on entire countries are almost always politically charged, peacekeeping is also an important aspect to consider in order to remove incentives to launch attacks in the first place.

Definition of Key Terms

Cyber warfare

Cyber warfare is "a series of strategic cyber attacks against a nation-state" ("What Is Cyberwarfare? | Fortinet"), which can cause severe harm. As mentioned in the introduction, attacks of this scale can cause damage, from disrupting infrastructure to losing life. Cyber warfare refers to the techniques used in a cyber war.

Cyber attacks

A cyber attack is a malicious and intentional attempt to breach the information system of an individual or organization. It is usually done because the attacker can benefit from infiltrating the information system, which is often monetary ("Hackers Think in All Directions. End-To-End Security Is the Answer.").

National Cyber Security Index (NCSI)

The NCSI is a global live index that measures how prepared a country is against cyber attacks and how effective and efficient a country is at managing incidents. This information is compiled by analyzing various factors in each country, such as regulations and documents. The NCSI also gives each country on its database a Digital Development Level (DDL) score. ("NCSI:: Methodology")

Anonymous

Hacker group Anonymous is a decentralized movement of digital activists known for launching cyberattacks against governments, companies, and other organizations with high profiles. It has no organizational hierarchy, and most of its activities are planned in encrypted messaging applications. Anonymous started on the imageboard 4chan and initially conducted cyberattacks and cyberbullying "for fun." However, after a successful large-scale cyberattack against the Church of Scientology in 2008, Anonymous stopped doing cyberattacks "for fun" in favor of digital activism, which this group pursues to this day. (Volle)

Denial-of-Service (DOS) and Distributed Denial-of-Service (DDoS) attacks

A denial-of-service (DOS) attack is a type of cyber attack where the attacker aims to render a device unusable by flooding it with so many requests that regular traffic cannot be processed. Unlike a DDoS attack, a DOS attack is launched from only one device. A distributed denial-of-service attack, however, is launched from many devices at once and sometimes employs a botnet (see below for more information). ("What Is a Denial-of-Service (DoS) Attack?")

Botnet

Occasionally referred to as a "zombie army," a botnet is a group of devices (usually hijacked and controlled using malware) used for cyber attacks and similar malicious purposes, most commonly spam or DDoS attacks. ("What Is a DDoS Botnet | Common Botnets and Botnet Tools | Imperva")

Background

Cyber warfare is complex due to its multifaceted nature. Attackers employ a wide range of weapons that must be accounted for in cybersecurity and damage control. Still, one must also analyze the political background to understand the attackers' motives. Damage control, resilience to incidents, and how technologically developed a country is are also important factors to consider for this issue.

Cyberattacks involved in the Russo-Ukrainian War (2013 to present)

Cyberwarfare has been a large part of the Russo-Ukraine confrontation since the Revolution of Dignity. For the past decade or so, the two countries have fired many attacks against each other, with Russia attacking Ukraine more. In this conflict, most cyberattacks involved are espionage or propaganda-related. (Mueller, et al.)

Russian cyber warfare activity:

The Russian Federation has launched a multitude of attacks against Ukraine during their still ongoing dispute. These include multiple power grid attacks, with the first one being the first-ever successful cyberattack conducted on a power grid. Russia also launched a series of powerful cyberattacks on Ukraine in June of 2017 using malware called NotPetya. (Greenberg and Excerpt) Said cyberattack is recognized as the most significant known hacker attack by the US Presidential Administration. The Russian Federation also has two identified hacker groups to its name. (editorialteam)

Ukrainian cyber warfare activity:

Ukraine has launched a significantly smaller amount of cyberattacks than Russia. They formed the IT Army of Ukraine in 2022, primarily to conduct cyberattacks against Russia. This organization has a unique hybrid structure that allows it to stay focused and purposeful. ("The IT Army of Ukraine | Strategic Technologies Blog | CSIS")

Estonia DDoS attack (2007)

In April of 2007, various Estonian institutions, such as media outlets and government services, were targeted by a DDoS attack. The Russian Federation made this attack to respond to the political conflict between the two countries involving the relocation of a World War II monument. Since Estonia was an early advocate for moving things online (e.g., elections), the attack was crippling and is often regarded as the first instance of cyber warfare, likely because this attack led to the creation of laws on cyber warfare ("Connect the Dots on State-Sponsored Cyber Incidents - Estonian Denial of Service Incident").

Major Parties Involved

Czech Republic

With a score of 98.33 on the NCSI, the Czech Republic is considered the most cyber-secure country in the world by the scale, with full marks in every category but militial cybersecurity. The Czech Republic sets the gold standard for cyber crisis management, cyber incident response, raising awareness for cyber threats, research and development of cybersecurity, and many more ("NCSI :: Czech Republic"). Their detailed 2023 cybersecurity report contains valuable information on how they achieved such good results for civilian cybersecurity, including details on future threats (e.g., quantum threat mitigation) and their education system and cybersecurity (Targets of Cyberattacks…Threats and Actors). The Czech Republic is exceptionally well-versed in cybersecurity, cyberattack defense, and education, which can be important as other countries can take inspiration from their solutions when writing their own.

United States of America

The United States of America (USA) is one of the most powerful countries in terms of technology. Not only does it have the largest GDP of any country in the world, as of April 2024 ("Countries with the Largest Gross Domestic Product (GDP) 2024 | Statista"), but the US also has a very high NCSI score of 84.17 (with perfect scores in various categories, such as military cyber defense, crisis management, and research and development) and is home to 8 of the ten most prominent tech companies in the world ("Largest Tech Companies by Market Cap"). This shows that the US is a technological superpower with massive resources. However, most US actions concerning this issue involve spreading awareness or removing malware, like in 2022 when they neutralized a Russian botnet and made their move public ("Significant Cyber Incidents | Strategic Technologies Program | CSIS").

Russian Federation

The Russian Federation plays a role differing from other large technological forces such as the US and China. It has a decent NCSI score of 71.53 and shows excellent scores in personal and military cybersecurity ("NCSI :: Russian Federation") (This information is from 2023, but judging by the almost linear graph of scores on the page, we can safely assume that the present score would not have changed much). Russia's teams of expert, politically motivated hackers make it incredibly relevant in this issue. These include the Kremlin-based hacker group Fancy Bear, which is responsible for many cyberattacks on Eastern European nations, and security-based organizations like NATO (editorialteam).

People's Republic of China

The People's Republic of China (PRC) has recently seen its economy shoot up to 2nd largest in the world, immediately behind the US ("Countries with the Largest Gross Domestic Product (GDP) 2024 | Statista"), and is home to tech giant Tencent. However, China's NCSI score is noticeably low, scoring a 0 in military cybersecurity and getting low scores in areas such as raising awareness and cybersecurity policy. China more than makes up for it with its powerful trade connections with the USA, with the majority of said trades being technology-related. The PRC also excels in education and research & development of technology. Overall, China holds an interesting stance on this issue but is nonetheless powerful and able to make improvements.

Timeline of Events

Date	Description of event
January 1, 1983	The Transfer Control Protocol/Internetwork Protocol (TCP/IP) is normalized, marking the birth of the Internet.
1996	The first DDoS attack is launched at Panix, an Internet service provider.
2004	Russian hacker group Fancy Bear is founded.
April 2007	Estonia faces a cyberattack by Russia, marking (what is widely considered) the first-ever instance of cyber warfare.
2009	In an act of cyber espionage, hackers accessed the Gmail accounts of Chinese human rights activists.

March 2015	China launched a cyberattack on GitHub, which was the largest DDoS ever at the time.
2016	Russia launches a cyberattack against Ukraine, targeting Kyiv's power grids. This is the first cyberattack to target physical infrastructure.
June 27, 2017	Sandworm, a Russian hacker group, sends NotPetya, a computer worm, to PCs worldwide, causing severe damages of up to $10 billion. (Greenberg and Excerpt)
December 2019	The COVID-19 pandemic has started, forcing most people to work from home / online. This hugely expands the amount of people vulnerable to cyberattacks.

Previous Attempts to Resolve the Issue

- **International Committee of the Red Cross (ICRC) rules of engagement:** In 2023, the ICRC published rules of engagement for civilian hackers based on international humanitarian law. These laws have been recognized and agreed upon by hacktivist parties such as the IT Army of Ukraine and, at one point, Anonymous. However, other parties, such as the Russian hacker group Killnet, ignored the rules. The ICRC also urges governments to place restrictions on hacking and work on law enforcement. In conclusion, the ICRC is making a valiant effort to, at the very least, lessen the risk of cyberwarfare.
- **Various United Nations General Assembly (GA) Resolutions:** Resolutions such as A/RES/58/199 and A/RES/55/63 of the General Assembly, particularly A/RES/58/199, deal with global cybersecurity, which can be very relevant to cyber warfare as well. Though GA resolutions are not legally binding, they contain many valuable solutions that may be considered by an extensive range of parties, especially since the GA has at least one representative from each member state. These resolutions cover a wide range of solutions, from research to crisis management, all of which can be chosen to be used by member states.

Possible Solutions

- **An educated approach:** When faced with a potential cyberattack, the most important thing to know is what to do, especially for large organizations like governments and high-profile corporations. Not having any education or inadequate education on cybersecurity means one is much more vulnerable to scams and attacks. Learning more about computer science and cyberattacks can also allow one to make better choices when purchasing antivirus and protection services.
- **Targeting the Root Cause:** Since cyberwarfare consists of politically motivated cyberattacks, a good solution could be targeting the root cause. By de-escalating political conflicts more efficiently and effectively, we can avoid or diminish the number of cyberattacks made due to said political conflicts. This can be done in several ways, e.g., by calling upon a third party like the International Crisis Group ("Crisis Group").

Bibliography

""Anonymous" Hacks Singapore Prime Minister's Website." *BBC News*, 8 Nov. 2013, www.bbc.com/news/technology-24862839. Accessed 24 Oct. 2024.

"A Brief History of the Internet." *Usg.edu*, 2024, www.usg.edu/galileo/skills/unit07/internet07_02.phtml. Accessed 15 Oct. 2024.

"Connect the Dots on State-Sponsored Cyber Incidents - Estonian Denial of Service Incident." *Council on Foreign Relations*, 2024, www.cfr.org/cyber-operations/estonian-denial-service-incident. Accessed 31 Oct. 2024.

"Countries with the Largest Gross Domestic Product (GDP) 2024 | Statista." *Statista*, 2024, www.statista.com/statistics/268173/countries-with-the-largest-gross-domestic-product-gdp/. Accessed 29 Oct. 2024.

"Crisis Group." *Crisisgroup.org*, 29 Aug. 2022, www.crisisgroup.org/. Accessed 30 Oct. 2024.

"Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats | Meetings Coverage and Press Releases." *Un.org*, 20 June 2024, press.un.org/en/2024/sc15738.doc.htm. Accessed 20 Oct. 2024.

editorialteam. "Fancy Bear Hackers (APT28): Targets & Methods | CrowdStrike." *Crowdstrike.com*, 2024, www.crowdstrike.com/en-us/blog/who-is-fancy-bear/. Accessed 31 Oct. 2024.

Greenberg, Andy, and Excerpt. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, 21 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed 30 Oct. 2024.

"Hackers Think in All Directions. End-To-End Security Is the Answer." *Cisco*, Aug. 2024, www.cisco.com/c/en/us/products/security/common-cyberattacks.html. Accessed 20 Oct. 2024.

"The IT Army of Ukraine | Strategic Technologies Blog | CSIS." *Csis.org*, 2023, www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine. Accessed 31 Oct. 2024.

Kaspersky. "A Brief History of Computer Viruses & What the Future Holds." /, 19 Oct. 2018, www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds. Accessed 15 Oct. 2024.

"Largest Tech Companies by Market Cap." *Companiesmarketcap.com*, 2024, companiesmarketcap.com/sgd/tech/largest-tech-companies-by-market-cap/. Accessed 29 Oct. 2024.

Mueller, Grace, et al. "Cyber-Operations During the Russo-Ukrainian War." *CSIS*, 13 Jul. 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Accessed 30 Oct. 2024.

"NCSI :: Czech Republic." *Ncsi.ega.ee*, 2016, ncsi.ega.ee/country/cz/. Accessed 28 Oct. 2024.

"NCSI :: Methodology." *Ncsi.ega.ee*, 2016, ncsi.ega.ee/methodology/. Accessed 20 Oct. 2024.

"NCSI :: Russian Federation." *Ncsi.ega.ee*, 2016, ncsi.ega.ee/country/ru_2022/. Accessed 29 Oct. 2024.

"OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats." *U.S. Office of Personnel Management*, 2023, www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/. Accessed 25 Oct. 2024.

Resolution Adopted by the General Assembly. 2004.

"Significant Cyber Incidents | Strategic Technologies Program | CSIS." *Csis.org*, 2024, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 29 Oct. 2024.

Targets of Cyberattacks National Cybersecurity Level Cybersecurity Trends for 2024 and 2025 2023 Report on the State of Cybersecurity in the Czech Republic Cybersecurity Threats and Actors.

Volle, Adam. "Anonymous | Definition, History, Purpose, Mask, & Facts." *Encyclopedia Britannica*, 2 Dec. 2022, www.britannica.com/topic/Anonymous-hacking-group. Accessed 24 Oct. 2024.

"What Is a DDoS Botnet | Common Botnets and Botnet Tools | Imperva." *Learning Center*, 20 Dec. 2023, www.imperva.com/learn/ddos/botnet-ddos/. Accessed 20 Oct. 2024.

"What Is a Denial-of-Service (DoS) Attack?" *Cloudflare.com*, 2023, www.cloudflare.com/learning/ddos/glossary/denial-of-service/. Accessed 20 Oct. 2024.

"What Is Cyberwarfare? | Fortinet." *Fortinet*, 2023, www.fortinet.com/resources/cyberglossary/cyber-warfare. Accessed 20 Oct. 2024.

"What Is Cyber Warfare | Types, Examples & Mitigation | Imperva." *Learning Center*, 20 Dec. 2023, www.imperva.com/learn/application-security/cyber-warfare/. Accessed 20 Oct. 2024.