GA1

The question of cyber security

German International School
of The Hague
Model United Nations

Sebastian Andersen

Forum: GA1

Issue: The question of cyber security

Student Officer: Sebastian Andersen

Position: President of the General Assembly 1

Introduction

The fear of cyberattacks has surged in the past decades and has grown into a threat, which can not be ignored in the modern world we live in. It first emerged in the 1960s when students of American universities hacked into the computers of their schools, but the real increase in the awakening, regarding the importance of good cyber security, happened in the 1980s with the commercialisation of the internet and the first cyber attacks on military software by foreign powers. These changes highlighted the creation of a entirely new space in which war could be raged and crimes could be committed. The cyber space.

The destructiveness of cyberattacks has been proven countless times in the last 20 years. In 2007 Estonia was hit by a chain of cyberattacks, mostly consisting of distributed denial of service (DDoS), after it was decided by the government to remove a statue commemorating the soldiers of the Soviet Union. This attack led to a halt in Estonian infrastructure, as banks, government facilities and various other organizations were hit, and resulted in Estonia briefly closing its digital boarders. A more recent example is the war in the cyber space, which plays out between Russia and Ukraine, simultaneous to the war on the physical level. Power grids and government communications methods have, for an example, been attacked multiple times, thereby hindering the war effort, crippling critical infrastructure and lowering moral, by targeting civilians in a way, which is not directly lethal.

Today this is, more than ever, a threat. Roughly 4.9 billion people, which makes up about 64% of the world’s population, has access to the internet and the world adapts to that. More and more public and military systems and services are moved into the cyber space, creating are more fruitful target environment for hackers with the intention of committing cybercrimes, but also for foreign armed forces, intending to gain a strategic advantage by securing information and weakening critical infrastructure, both military and civilian. This increases the need for a good cyber security, in order to prevent unintended breaches of important systems and the disclosure of confident information.

Definition of Key Terms

Hacking
The fraudulent proses of gaining access to data in a digital system, with harmful intentions.

Cyber warfare
Hacking of computer systems, which contain military or political information and thereby giving the hacking side an advantage. An example for this is the targeting and disruption of both military and civilian infrastructure.

Cyberespionage
Hacking of computer systems of governments, companies and other such, for the sole purpose of gaining information.

Cyberattack
An attempt from hackers to breach a computer network or system, in order to damage or destroy it. If such an attack is state sponsored, a certain government has financed the action, in order to gain an advantage, mostly targeting geopolitical competitors.

Internet
A computer network, which links people together through their digital devices.

Hardware
The physical parts of a computer system

Software
The instructions, which dictate the use and capabilities of a computer systems.

World wide web
A platform on the internet, making communication between people easier and simpler, than it previously was.

Virus
A computer code, written with the sole purpose of copying and spreading itself to as many networks as possible, to cause as much disruption and damage as possible.

Malware
Software design to gain unauthorized access and harm a computer network or system.

Zero-day vulnerabilities
A term used to describe a security flaw in a soft- or hardware system, which is unknown to the developer or vendor and therefore poses a great risk to the security of the system.

Distributed Denial of Service (DDoS)
An attempt to disrupt a system in a way, in which it will no longer be able to offer the service it was intended to.

Phishing
A fraudulent attempt to obtain secret or private information from a computer system or network.

Botnet
A net of computers infected by malware and used by hackers to cause more harm and disruption.

General Overview

Cyber security refers to the safety of a digital system against cyberattacks of all origins. Such attacks are defined as a computer based attempt to gain access, disrupt or even destroy a second system.

The three layers of cyberspace
The cyberspace is composed of three layers, which can be attacked using different methods. The first layer is the physical layer, which consists of hardware, satellites and other physical components. Software, providing the operating instructions for the physical equipment, belongs to the second layer, also called the syntactic layer, and is the most targeted layer in regards of cyberattacks. The third layer, called the sematic layer, composed of the human, which interacts with the system or network.

Different types of cyberattacks
Cyberattacks can take many different forms. The most prominent attack method, is the DDoS, which floods a system or network with requests, in order to overload the system and thereby incapacitating it. This is often conducted with the aid of a botnet. Another prominent form of cyberattack is the phishing of vital information, in order to gain an advantage over the sematic layer of the cyberspace.

Different uses of cyberattacks
The motivation for cyberattacks can be numerous and it is vital to acknowledge and identify these in order to respond and combat the attacks properly.

Cyber warfare

Cyber warfare refers to the use of computer-based technologies and techniques to carry out offensive or defensive operation to disrupt, damage or gain access to a digital system, network or data, conducted by states, state-sponsored or state-affiliated groups. It is waged in order to achieve a military, geopolitical, economic or other strategic advantage or objective. Cyber warfare can be directed at the physic and sematic layer by attacking the hardware and the operator or at the syntactic layer, when the software of a system or network is being hacked.

Cybercrime

Cybercrime is conducted by criminal groups, which are not affiliated with any sort of government or country. It can take many forms, but one of the most prominent is the hostage taking of a system. With this method the group or the single hacker takes over a system or network, often those of big cooperations and companies, and demands a ransom in order to give back the control to the original owner. These ransoms have been increasing, especially in the last couple of years. For an example was the average ransom around 812,000$ in 2022 but in 2023 this has increased to around 1.54 million dollar.

Cyberespionage

Cyberespionage can be closely affiliated with cyber warfare, as it is used by states, state-sponsored or state-affiliated groups to gain information on geopolitical enemies, without being detected or causing direct harm to the country under attack. The most used method is phishing.

Cyberterrorism

Cyberattacks have also become a prominent method of terrorism. Cybercrime is used to finance various terroristic activities, whilst other attacks are directly involved in terrorism or an instrument of such. An example of this is Ardit Ferizi, who was charged with cyberterrorism by the Department of Justice of the United States of America (USA) in 2016, after he hacked into a military site, stole data and sold this to the terrorist group Islamic State of Iraq and Syria (ISIS).

The importance of cyber security

The importance of cyber security can not be stressed enough. Without sufficient cyber security a country is vulnerable to attacks, which could aim at, but not limited to, disrupting critical infrastructure, sowing confusion amongst the population or the theft of vital and possibly secret data. Examples of such attacks have been numerous in the past 20 years with variations in the outcome, depending on the cyber security system of the country under attack. For an example did the attack on a Ukrainian energy cooperation in 2015 leave around a quarter of a million people

with out power, whilst an attack on the Israeli water system failed, without causing much harm to the people of Israel. The protection of individual people against cyberattacks is also of the utmost importance, as it is the governments responsibility to protect the privacy and the wellbeing of their citizens. It is due to these reasons, that the issue of cyber security holds so much importance and therefore should be solved by means of international cooperation.

Major Parties Involved

International Telecommunication Union

The International Telecommunication Union is an organization of the UN, which specialises on information and communication technologies (ICT). In regards to cyber security the ITU works on facilitating international agreements, helps countries and organizations establish a cyber security system and ensures dialog.

United Nations Office on Drugs and Crime

One of the countless tasks of the United Nations Office on Drugs and Crimes (UNODC) is the field of cybercrime and measures to limit and eradicate the issue. The office provides aid, spreads awareness, conducts research and insures international dialog.

United Nations Office of Counter-Terrorism/United Nations Counter-Terrorism Centre

The United Nations Office of Counter-Terrorism (UNOCT) and the United Nations Counter-Terrorism Centre (UNCCT) focuses on cyberattacks with connections to terrorism, whether these attacks are used to commit, fund or recruit for terrorist activities.

Russia

The Soviet Union, predecessor of many member states including Russia, was the first country to make use of cyber-attacks in the 1980s, when they hacked into American military systems. Russia has since then proposed a international code of conduct for information security, in cooperation with China, Tajikistan and Uzbekistan, but it failed to attract global support. From 2009 till 2018 27.2% of all cyberattacks originated from Russia, whilst it is suspected that Russian groups have conducted 164 state sponsored attacks since 2005. Furthermore, there is evidence, that Russia host various hacker groups, such as Cozy Bear.

China

China was one of the co-submitters of the failed code of conduct, proposed in 2011. Meanwhile 28.6% of cyberattacks between 2009 and 2018 have their origins in

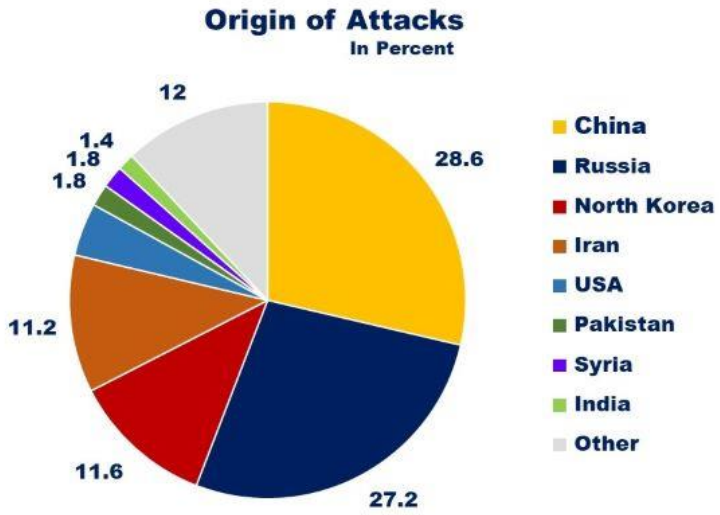
China. In addition to this it is suspected that China was involved in 241 state sponsored cyberattacks, whilst maintaining the largest cyber army in the world.

Iran

Iran is another country, from which a substantial amount of cyberattacks originate. It is also suspected that the government makes extensive use of state sponsored cyberattacks, with 92 being suspected between 2005 and 2022.

United States of America

In the first half year of 2023 approximately 85.6 billion threats were blocked by American cyber security systems, making the United States of America (USA) the most targeted country in the World. Meanwhile the USA is suspected of conducting 20 state sponsored cyberattacks from 2005 onwards.



Origin of Cyberattacks between 2009 and 2018, BIIA, https://www.biia.com/cyber-security-statistics-440-increase-in-global-documented-attacks-from-2009-to-2018/cyber-attacks-origin-1-2/

Timeline of Events

Date	Description of event
1962	The idea of ARPAnet, an early military version of the internet, was proposed and developed.
late 1960's	The, until then, strict military-only system was made available for universities.
late 1960's	Students "hack" university computers.

1969	Invention of the Internet.
1980's	Markus Hess, a German hacker, hacks over 400 US-military computers for the KGB. This is believed to be the earliest attempt to use hacking for military advantages.
1982	The first worldwide spreading virus was written by a 15-year old, infecting the Apple-II computers.
1985	First attacks, via the internet.
1988	Morris Worm becomes the first person to be convicted for hacking.
1989	The invention of the world wide web, makes it possible for people to connect on larger scales all over the world.
1998	First Resolution on the topic of cyber warfare passes (A/RES/53/70).
1999	Teenagers hack the American department of defence and NASA, thereby proving the vulnerability of all government facilities.
November 23rd 2001	The Budapest Convention is approved.
2004	The Budapest Convention is adapted.
2004	The Group of Governmental Experts (GGE) is formed, in order to monitor and report activities regarding cyber warfare. The group is till this day a major factor in the fight against cyber warfare, in the United Nations.
2007	Estonia becomes the first country to be hit by a cyber offensive, mostly comprised of DDoS. This follows a dispute between the Estonian and Russian government over the movement of a statue. Some have called it Cyber War 1.
2009	A mass cyber offensive on American companies, named operation Auora, is launched by the Chinese government. These companies include the technology company Google, defence contractor Northrop and Grumman and many others.

April 2010	A proposal for a global treaty on cybercrime is rejected, due to a failure in reaching an agreement between less economic developed countries (LEDCs) and more economic developed countries (MEDCs).
September 14th 2011	China and Russia propose an international code of conduct for information security, but found little global support.
June 2013	Confidential NSA information is leaked by Edward Snowden.
2015	The cyber-attacks on power grids belonging to the company Prykarpattyaoblenergo, in Ukraine, marks the first cyber-attacks on power grids. About 230,000 people were left without power for one till six hours.
24th of February 2022	Russia invades Ukraine, completely changing the security situation in Europe. The invasion was preceded by a large cyber offensive on Ukrainian military and civilian infrastructure.
After 24th of February 2022	Russian cyber-attacks on Ukrainian computer network and systems continue, for an example have official government websites been hit multiple times. This proves and illustrates the role of cyber warfare in modern warfare.

Previous attempts to solve the issue

Previous attempts at solving the issue of cyberattacks have been numerous. From the beginning of the digital age in the 1970s governments and cooperations alike have been establishing their own cyber security measures, in order to protect the national and cooperate cyber space.
In addition to this the UN tasked various offices and organizations with the improvement of the issue. For an example is the ITU tasked with the general improvement of global cyber security, whilst offices such as the UNODC, the UNOCT and the UNCCT have been focused on more specific areas of the issue. The responsibility of the UNODC is to monitor and aid with the combat against cybercrime, whilst the UNOCT and the UNCCT are tasked with similar task regarding the cybercrimes surrounding terrorism.
The will of the United Nations to combat cyber attacks has also been outlined in various resolutions of the past. Starting with the resolution regarding developments in the field of information and telecommunications in the context of international security (A/RES/53/70), which was passed in 1998 and marked the crucial beginning

in the improvement of international cyber security. Other important resolutions on the issue were the resolution regarding the creation of a global culture of cybersecurity and the review of national efforts to protect critical information infrastructures (A/RES/61/211) or the Delhi declaration by the United Nations Security Council (UNSC), which aimed at increasing cyber security toward attacks with terroristic intentions. In addition to this the Budapest Convention was signed in 2004 by 50 countries, aiming at decreasing cybercrime. This should be done with different methods, for an example by harmonizing the laws of signatory states to increase the effectiveness of the global fight against cybercrime.

Possible Solutions

As a first step to increase cybersecurity, it is vital that all governments acknowledge the threats from cyberattacks and that there can be waged war in the digital as well as the physical world. By creating a unified position on the issue, the strive for an active solution increases massively and becomes increasingly constructive.
After this step it is important to establish a certain framework and code of conduct for warfare in the digital world, similar to the role the Geneva Conventions play in physical warfare. Such rules and regulations could be decided upon at an international conference, dedicated to this sole purpose.

Furthermore, international cooperation against cybercrime could be strengthened. This could be done with various methods, such as, but not limited to the sharing of relevant data, united investigations in relevant cases or the establishment of an annual conference, at which the countries share experiences, successes and problems, whilst trying to increase the effectiveness and cooperation in the field of cybersecurity in the following year. In addition to the to increased international cooperation, member states could also focus on the expansion of cooperation with the private sector. With the help and the knowledge of the private sector it would be possible to bolster the cyber security of both the public and private cyber space. Special attention should also be devoted to less developed countries (LDCs) and to Micro-, small- and medium-sized Enterprises, as these often lack the resources, capacity, frameworks and awareness, which are required for an effective cyber security system. Aid could be provided by an combination of more developed countries (MDCs), the UN and Non-governmental organizations (NGOs)
Current UN Programmes could also be restructured in order to establish one specialized office or organization focused on all aspects of cyber security. This organ of the UN would still be responsible for the same tasks as the offices and organizations now, but would be concentrated in one place and be able to aid governments more effectively, by being the expert group on all dangers of the cyberspace.

Bibliography

Developments in the field of information and telecommunications in the context of international security, United Nations, accessed 7th of December 2023, <Developments in the field of information and telecommunications in the context of international security – UNODA>

The Morris Worm, 2018, FBI, accessed 9th of December 2023, <The Morris Worm — FBI>

The Budapest Convention (ETS No.185) and its Protocols, Council of Europe, accessed 9th of December 2023, <Budapest Convention - Cybercrime (coe.int)>

The invention of the Internet, History.com editors, 2019, HISTORY, accessed 15th of December 2023, <The Invention of the Internet - Inventor, Timeline & Facts (history.com)>

Cyberwar, John B. Sheldon, 2023, Britannica, accessed 15th of December 2023, <Cyberwar | Cybersecurity, Cyberattacks & Defense Strategies | Britannica>

Cyber Warfare: An Evolution, Phillip Lu, 2016, Roskilde University, accessed 15th of December 2023, <GRP_#6__Cyber_Warfare_An_(ruc.dk)>

A short story about the web, CERN, accessed 15th of December 2023, <A short history of the Web | CERN (home.cern)>

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, United Nations, accessed 17th of December 2023, <Ad Hoc Committee - Home (unodc.org)>

Regional Perspectives on Cyber-Security: Formation and Evolution, Stelian Dumitrache, Christopher Jolliffe, Sandra Rector and Oliver Woodhall, 2017, Oxford University, accessed 17th of December, <oxford-berlinteamcybersecuritypdf>

Russia's war on Ukraine: Timeline of cyber-attacks, Jakub Przetacznik and Simona Tarpova, 2022, European Parliament, accessed 17th of December 2023, <Russia's war on Ukraine: Timeline of cyber-attacks (europa.eu)>

What is cyber Cybersecurity, Cisco, accessed 17th of December 2023, <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

Estonian denial of service incident, 2007, council on foreign relations, accessed 17th of December 2023,< https://www.cfr.org/cyber-operations/estonian-denial-service-incident
>

Cybersecurity and New Technologies, United Nations Office of Counter-Terrorism, accessed 17th of December 2023, <https://www.un.org/counterterrorism/cybersecurity>

Role of ITU in building confidence and trust in the use of ICTs, ITU, accessed 19th of December 2023, <https://www.itu.int/en/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx#:~:text=ITU's%20contribution&text=This%20includes%20facilitating%20agreement%20on,capacity%2C%20and%20facilitating%20policy%20dialogue>

Cybercrime, United Nations Office on Drugs and Crime, accessed 19th of December, <https://www.unodc.org/romena/en/cybercrime.html>

Brazil is the worlds second most vulnerable country to cyberattacks, Angelica Mari, 27th of September 2023, Forbes, accessed on the 19th of December 2023, <https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/>