DISEC

18

Issue Description

KarMUN 2024 Global Consciousness

COMMITTEE	Disarmament and International Security Committee
ISSUE	The Issue of Regulating Cyber Warfare
SUBMITTED BY	Laura Finch, Viktória Gyuricza, Nóra Kutas, Chairs of the Disarmament and International Security Committee
APPROVED BY	Szófia Tóth, President of the General Assembly

Introduction

Cyberwarfare is the use of computer technology to disrupt the activities of a state or organisation. Most of the threats are targeted attacks, which can escalate rapidly and quickly “reach the threshold of national security”. This is why international cooperation is vital when discussing cyber threats as well as when preparing nations for possible threats.

Over recent years, cyberspace has become more and more open and has been increasingly impacting our lives, therefore, more nations are considering cybersecurity “as a national security priority”. The level of preparedness and willingness to cooperate depends on political actors, as international cooperation can only be reached if countries set their own laws concerning cyber security. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) has conducted research on countries’ response to cyber threats, and their ways of implementing policy changes for protection against threats. The findings, outlined in the National Cyber Security Framework, show that in order to formulate a comprehensive and effective strategy, a number of factors must be taken into consideration; this includes international organisations, lawmakers, and law enforcement agencies as well as infrastructure providers. All of these areas should be in cooperation to communicate, formulate, and implement new policies. The European Union has also put forward a strategy to combat cyber threats and attacks and protect citizens. It aims at outlining the principles of cybersecurity, ways of achieving cyber resilience, and developing a cyber defence policy.

Definition of Key Terms

Cybersecurity - The art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Cyber warfare - The use of technology to disrupt the activities of a state or organisation, especially the deliberate attacking of information systems for strategic or military purposes.

Cyber operations - The activities of gathering evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or support other intelligence activities.

Hacktivism - The act of hacking or breaking into a computer system for politically or socially motivated purposes.

Automated (bot) accounts - Inauthentic accounts that imitate the tasks and actions of users and are usually used for nefarious purposes (eg: spreading spam)

Information warfare - The act of conducting an operation in order to gain an information advantage over the opponent.

General Overview

HISTORY

There are multiple debates on the term 'cyber warfare' as most agree 'cyber crime, espionage or terrorism'. This is justified by the general observation that a cyber attack committed by one state against another does not necessarily result in war between the countries but mainly increases tensions. In addition, issues of cybercrime are usually fought by law enforcement or legislation instead of the military. However, it is "widely believed" that cyber crime will play an increasingly important role in conflicts in the future, therefore, it is vital to understand it and create frameworks for both the regulation of cybercrime and response to such attacks.

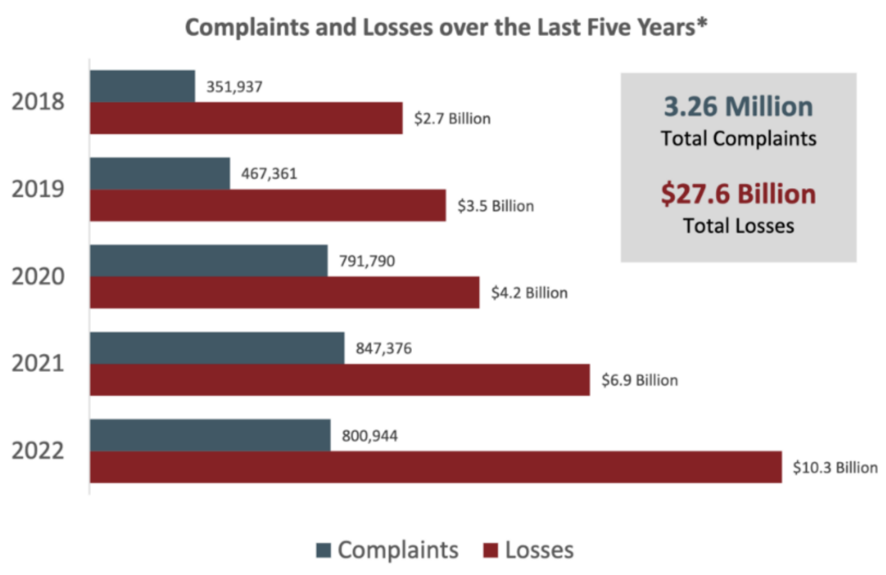
The earliest cyber crime was committed in 1834, before the invention of the Internet, where two attackers in France stole data from a financial institution. Later, in 1971, when the first virus was developed, it served as a warning for how dangerous cyber attacks could become in the future. During the Cold War, technology developed quickly in the USA and Soviet Russia, as apart from the arms race they were also racing to create new technological developments. By the 2010s cybercrime was escalating and now millions of people and great amounts of money and assets were at stake.

Some notable cyber attacks include Russian interference in the 2016 American elections as well as the Brexit referendum in the United Kingdom. In 2016, an article was posted in the Washington Post, showing that a cybersecurity firm (CrowdStrike) had found evidence of outside influence. It states that Russia helped Donald Trump to be elected through "active measures". In the UK, David Cameron was on record saying that Russia "might be happy" with Brexit happening, and later documents were published stating that the collapse of the voting page was believed to be caused by foreign interference. However, there is no direct evidence to support these claims.

Because of the advances in technology, attackers are increasingly using AI to interfere with systems and organisations. Therefore, it is increasingly difficult to "stay one step ahead" which is why VPNs and other protective measures as well as EU and political schemes are being developed.

Cyber attacks have a profound impact on the targeted organisations, which include financial loss and damaging reputation. In some cases, businesses have to pay in order to regain access to stolen information or have profit losses because of websites being down for longer periods (this can also result in a "decline in customer loyalty").

GRAPH: DAMAGE CAUSED BY CYBER CRIME IN RECENT YEARS (USD)



HOW DOES CYBER WARFARE WORK

According to the National Cyber Security Centre (NCSC) (in the UK), there are two main types of cyber attacks: targeted and untargeted. The untargeted attacks are not focused and do not target specific individuals or businesses. They consist of sending out multiple viruses, compromising websites or attacking random parts of a server or the internet.

Targeted cyber attacks, on the other hand, are carefully crafted and carried out. The planning (survey) stage of the attack could take months to develop and consists of obtaining valuable information about the target and identifying potential vulnerabilities. The next stage is “delivery” where one of the vulnerabilities in a system can be exploited, and “breach” is the action of “making changes that affect the system’s operation”. The “effect” stage is the last, where attackers achieve their goals, which could be to establish a continuous presence, retrieving information they wanted access to or setting up payments to a bank account they control.

TYPES OF CYBER ATTACKS

There are numerous different types of cyber attacks, of which malware, phishing, smishing, and vishing are the most common. Malware is a virus or other code-based program which is usually downloaded by users unknowingly and thus spreads on the device to steal private information. One of the types of malware is spyware, which is similar to malware in the sense that the attacker’s aim is to get access to information, however, in this case, the presence of the attacker remains unknown.

Phishing is a technique used by hackers which is used to get information from the user by demanding sensitive or personal details. In this case, the attacker would send an email or message with a link, and when the user clicks on it, malware is installed on the computer and details are stolen. Smishing has the same effect, but the attacker conducts the attack via text or phone call in the case of vishing.

In all of these cases, attackers are attempting to steal important information from the users. In many instances, these details are later sold on the dark web or, alternatively, collected and used in a larger-scale cyber attack or crime.

TYPES OF CYBER WARFARE ATTACKS

According to the data protection tool, Imperva, there are seven main types of cyber warfare attacks. Firstly, espionage refers to the monitoring of a country in order to steal secrets.

Second, sabotage refers to the act of leveraging or exploiting insider threats (careless or dissatisfied employees) to steal or destroy information.

Third, Denial-of-service (DoS) attacks aim to stop users from getting to a website by flooding it with information or requests.

Fourth, attacking the power grid aims to collapse communications, disrupt critical infrastructure and systems and this can also result in bodily harm. This is effective because by cutting communication and the internet, it becomes difficult for parties to communicate and solve the problem.

Fifth, propaganda attacks are meant to influence how people think on a certain topic or issue. It is often used to expose the truth or spread false information to trick citizens into losing faith in their country.

Sixth, economic disruption happens when an attacker targets a computer network of an economic establishment which can render the economy or financial markets exposed and vulnerable even for longer periods of time.

Seventh, a surprise attack, which is used mostly as a base for a physical attack. This is called hybrid warfare, when cyber and physical attacks are used simultaneously or to help each other.

PROTECTION AGAINST CYBER ATTACKS

Probably one of the most effective ways of fighting against cybercrime is by staying educated and being aware of potential risks. In addition, it is important to change passwords and usernames and store information in a secure location.

Firewalls and anti-virus scans can also be useful. The main aim of firewalls is to protect a device from attacks in the first place. If this is no longer possible, an anti-virus scan can be run in order to determine whether there is malicious activity on a device, and in some cases, this software removes the possible malware as well.

Cyber attacks can target states, companies, and individuals but in any case, it is important to be prepared. Countries should have a framework in place to combat cyber attacks and keep citizens safe. Organisations can implement plans and regular training which can also help employees on a personal level. Cyber warfare is made up of multiple cyber attacks on organisations or individuals

Major Parties Involved

Russia: Russia has participated in multiple cyber attacks against governments as well as individuals or enterprises.

Ukraine: As a former part of the Soviet Union, Ukraine has been affected by cyberattacks from Russia on a number of occasions.

United Kingdom: Similarly to the USA, the UK has also been a victim of multiple cyber attacks (most notably the possibility that Russia interfered in the Brexit referendum of 2016) but they are also a leading force in technological development.

People's Republic of China: China has been accused by multiple countries for cyber threats and attacks. There have been multiple attacks on the USA since the beginning of the 2000s (for example, attacks on US Navy bases, Google, other tech companies, and newspapers.

Taiwan: Taiwan has been an area of interest for China for a number of years which has resulted in numerous cyber threats.

Democratic People's Republic of Korea: The Lazarus Group is based in Korea and is believed to be responsible for a number of attacks between 2010 and 2021. Targeted countries include Bangladesh, the USA as well as North Korea.

United Arab Emirates: The UAE has experienced 71 million cyber attacks in 2023 according to Dr Muhammad Al Kuwaiti, the head of the Cybersecurity Council. There have been harsh penalties introduced and programs implemented to fight off attacks.

United Nations Institute for Disarmament Research (UNIDIR): an institute within the UN that conducts "research on disarmament and security". The main areas of focus are nuclear weapons, artificial intelligence, chemical and biological weapons, missiles and drones as well as conventional weapons.

United Nations Office of Counter-Terrorism: an institute within the UN which "leads and coordinates" approaches and actions to counter terrorism and violent extremism.

Human Rights Watch (HRW): a non-governmental organisation which aims to investigate and report human rights violations around the world.

Stop Killer Robots: a group of non-governmental organisations campaigning for the banning of lethal autonomous weapons.

Timeline of Events

2 November 1988 - The first ever internet computer worm, the “Morris worm” was made.

1998 - Cyber Attack as a concept is first referred to publicly by CIA Director George Tenet.

29 June 1999 - Jonathan James got inside the US Department of Defense (DOD) computers and installed a backdoor within its servers. He later stole NASA software used to support the International Space Station.

April 2007 - Estonia experienced what is believed to be the first cyber attack targeting an entire nation. 58 Estonian websites went offline including government, bank and media websites.

November 2008 - Foreign intruders used “thumb drives”, portable memory sticks, to infect DOD networks, leading to what a Pentagon official later described as the “most significant breach of US military computers ever”.

August 2010 - The Pentagon officially recognizes cyberspace as a “new domain of warfare”.

December 2011 - The US Chamber of Commerce network was penetrated by hackers for over a year, allowing access to member company communication and industry positions on US trade policy. The hackers were later linked to the China’s People’s Liberation Army.

May 2017 - The WannaCry ransomware encrypted data on victims’ computers and demanded a ransom payment in order to decrypt the data. This attack affected more than 200,000 computers in 150 countries.

June 2019 - Russia interfered with the Brexit referendum in the UK, supporting members who wanted to separate from the EU.

Previous Attempts to Solve the Issue

During the past decades there have been multiple attempts to regulate and defend against cyber attacks. As of now almost every country in the world is equipped with a cyber defence system. Cybersecurity, which includes firewalls, intrusion detection, login passwords, prevention systems and many more, is now everywhere.

Significant actions taken to prevent cyberattacks:

- **2003** – The Department of Homeland Security consolidates several cyber defence offices to form the National Cyber Security Division (NCSD), aiming to protect government computer systems from internet-based attacks in the USA.

- **14 May 2008** – NATO's cyber defence centre the Cooperative Cyber Defence Centre of Excellence (CCDCOE) was formed.

- **October 2009** – new National Cybersecurity and Communications Integration Centre (NCCIC) opens in the USA, which is a 24-hour "watch and warn" centre.

- **January 2011** – Estonia establishes a "Cyber Defence Unit" within the Estonian Defence League, comprising volunteer scientists and other members who, in times of war, would operate under military authorities.

- **September 2015** – The Chinese President Xi Jinping and American president Barack Obama met and discussed issues related to cybersecurity and reached a preliminary agreement.

Besides these many organisations, both governmental and non-governmental (NGO) such as the International Association of Cybercrime Prevention or the Cyber Peace Foundation, provide information, raise awareness and counsel education and training in favour of providing security on a global level.

Possible Solutions and Approaches

One possible approach is promoting International Cooperation and Agreements. The increasing frequency of cyber threats necessitate a collective and collaborative approach among nations. International cooperation can foster the creation of standardised protocols for incident response, information sharing, and the investigation of cybercrimes.

Another essential action is to support capacity-building efforts, especially in developing countries, to enhance their ability to prevent and respond to cyberattacks. As these threats become more and more common, cyberspace professionals and law enforcement agencies must equip themselves with the necessary skills and tools to identify and prevent cyber attacks.

Promoting cybersecurity education and awareness programs to the general public and smaller businesses can also be helpful. Being informed about cyber threats is crucial in today's world where everyone depends on technology. Education empowers individuals to adopt responsible online behaviours, recognize phishing attempts, and implement robust security practices.

It's important to note that regulating cyber warfare requires a multi-stakeholder approach, involving governments, private sector entities, international organisations, and the broader global community

Bibliography:

Carter, Lisa, and Lisa Carter. “10 Biggest Cyber Attacks in History | Clear Insurance.” Cyber Attacks Are on the Rise. Whilst Modern Technology Presents Many Conveniences and Benefits, There Are People Who Misuse It Which Poses a Threat to Businesses and Data Privacy Globally. When Data Breaches Happen, It Can Have a Far-reaching Impact. It Goes Beyond the Target Company, Affecting Customers, Suppliers and More. Scarily, Experts Expect The, June 18, 2023. https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/.

“EUR-LEX - 52013JC0001 - EN - EUR-LEX,” n.d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.

Fortinet. “Top 5 Most Notorious Attacks in the History of Cyber Warfare | Fortinet,” n.d. https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare.

Hoory, Leeron. “What Is a Cyber Attack? Definition, Types & Prevention.” Forbes Advisor, August 14, 2023. https://www.forbes.com/advisor/business/what-is-cyber-attack/.

Kamen, Dan. “What Is a Cyber War – Explained.” NEIT, July 5, 2023. https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=The%20history%20of%20cyber%20warfare%20goes%20back%20to%20the%201980s,digital%20warfare%20and%20espionage%20increased.

Kovacs, Eduard. “Cybercrime Losses Exceeded $10 Billion in 2022: FBI.” SecurityWeek, March 13, 2023.
https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/.

Nakashima, Ellen. “Cybersecurity Firm Finds Evidence That Russian Military Unit Was behind DNC Hack.” Washington Post, April 12, 2023.
https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?postshare=9631482406341944.

“Office of Counter-Terrorism |,” n.d.
https://www.un.org/counterterrorism/#:~:text=Across%20the%20globe%2C%20the%20United,counter%20terrorism%20and%20violent%20extremism.

Sheldon, John B. “CyberWar | Cybersecurity, Cyberattacks & Defense Strategies.” Encyclopedia Britannica, January 4, 2024.
https://www.britannica.com/topic/cyberwar.

UNIDIR → Disarmament Is Evolving. “UNIDIR | Building a More Secure World.,” n.d.
https://unidir.org/.

United Nations. “Towards Cyberpeace: Managing Cyberwar through International Cooperation | United Nations,” n.d.
https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

Wikipedia contributors. “Cooperative Cyber Defence Centre of Excellence.” Wikipedia, January 26, 2024.
https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence.

Wolf, Arctic, and Arctic Wolf. “A Brief History of Cybercrime.” Arctic Wolf, October 19,2023. https://arcticwolf.com/resources/blog/decade-of-cybercrime/#:~:text=Technically%2C%20the%20first%20cyber%20attack,accessing%20the%20French%20telegraph%20system.

“Xi Jinping, Obama Talk Cybersecurity,” n.d. http://america.aljazeera.com/watch/shows/live-news/2015/9/xi-jinping-obama-talk-cybersecurity.html.

FURTHER RESOURCES

US policy:
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

US Annual Threat Assessment
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Cybersecurity Policies
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Foreign Policy Responses to International Cyber-attacks (Netherlands)
https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

Top countries best prepared against cyberattacks
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Top-countries-best-prepared-against-cyberattacks.aspx

France cybersecurity strategy
https://www.globaltradealert.org/intervention/101617/state-loan/france-government-launches-cyber-security-strategy#:~:text=On%2018%20February%202021%2C%20the,cyber%2Dsecurity%20solutions%20in%20France.

Iran Cyber Threat Overview and Advisories
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

Cyber Security Organisation Spain
https://ccdcoe.org/library/publications/national-cyber-security-organisation-spain/

Russian Cyber Attacks and Warfare
https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia#

Chinese Cyber Attacks and Warfare
https://en.wikipedia.org/wiki/Cyberwarfare_by_China

The Lazarus Group
https://en.wikipedia.org/wiki/Lazarus_Group

Cyber Attacks in the UAE
https://www.thenationalnews.com/uae/2023/11/03/uae-has-thwarted-71-million-cyber-attacks-this-year-authorities-say/

Joint Framework of the European Parliament on countering hybrid threats
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

Managing cyberwar through international cooperation
https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

UNOCT
https://www.un.org/counterterrorism/#:~:text=Across%20the%20globe%2C%20the%20United,counter%20terrorism%20and%20violent%20extremism.

UNIDIR
https://unidir.org/

HRW
https://www.hrw.org/

CCDCOE,
https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence

Stop Killer Robots
https://www.stopkillerrobots.org/

https://www.nato.int/cps/en/natohq/topics_156338.htm

https://www.hnmun.org/nato-2023

https://www.lawfaremedia.org/article/legal-aspects-hybrid-warfare

https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250

Washington Post, Russian interference in the 2016 elections
https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?postshare=9631482406341944

Timeline of cyberwarfare:
https://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline