Futuristic Security Council

Cyber Warfare and global security

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Danyal Mohammed

Forum	Futuristic Security Council
Issue:	Cyber Warfare and global security
Student Officer:	Danyal Mohammed
Position:	Head Chair

Introduction

The modern world is a changing and developing place. A major source of this change can be attributed to the groundbreaking and fast paced developments of technology in the last half century. It can be argued that almost every aspect of life, whether good or bad, has been impacted by the development of technology within this period. This report covers modern developments in warfare and the digital worlds' increasingly exponential role in the threat to global security and peace. Cyber warfare, from an innovation perspective could be described as the artificial intelligence of the military world. A constantly changing and not yet fully understood aspect of military strategy. Officially, cyber warfare is defined by the Oxford English dictionary as "the use of computer technology to attack a state or organization's information systems, potentially disrupting critical functions". Due to cyber warfare's rapidly changing nature it becomes hard to predict and take long term measures against cyber warfare. Most solutions to prevent a cyber attack consist mostly of short-term pre-emptive measures and quickly developing solutions to newly created cyber attacks. Luckily, the motivation for cyber attacks as we know them today are often classified into a few categories: espionage, sabotage, denial of service attacks, attacks on infrastructure, propaganda, attacks targeting the economy and so called "Surprise attacks". Each one of these motives for cyber warfare threaten global security in their own way and will each be discussed in more depth later. As of today, not every country in the world has the logistical capabilities to execute a cyber attack, limiting the number of key players capable of cyber warfare, despite this however, every country can receive a cyber attack due to vast worldwide connection offered by the internet which is a common basis for cyber attacks. This truly reflects the global need to implement measures against cyber attacks to keep the world more secure.

Definition of Key Terms

Social engineering

Social engineering is a manipulation technique that exploits human error to gain private and valuable information or access. Used in more vulnerable countries or individual companies with low cyber literacy.

Phishing

Phishing refers to a coercive attempt to steal sensitive information or other important data in order to utilize or sell the stolen information. Used on individuals or organisations to take personal information in a cyber attack.

Distributed Denial of Service (DDos)

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt internet traffic of a server, service or network by overwhelming it by flooding it with data. Used on individuals or organisations with limited digital infrastructure.

Ransomware attack

A Ransomware attack is a type of malware which prevents you from accessing your device and the data stored on it. Often requiring money or a service to retrieve the data. Could be thought of as “holding data hostage”. Specifically targeting organisations or government agencies with large amount of strategically useful data.

Black hat hacking

Hacking for a nefarious purpose or with bad intent. Considered illegal internationally, often executed outside of employment targeting countries and individuals.

General Overview

Cyber-Espionage

Espionage is one of many forms of warfare which in recent years has been digitalised with the rise of the internet and is further traveling down this trajectory of modernisation with the developments of artificial intelligence; in fact 25% of cyberwarfare today consists of cyber-espionage.

Like many other motivations for cyber warfare, there is no telling in which direction espionage will turn in regard to new developments in its cyber sector. This is mostly due to the aforementioned rapid developments of technology and digitalising of military strategies. Espionage is officially defined as the “process of obtaining military, political, commercial, or other secret information by means of spies, secret agents, or illegal monitoring devices”. The “spies, secret agents, or illegal monitoring devices” are all aspects of espionage that have been recently and continue to be digitalised. On top of this multiple new techniques in cyber espionage have been developed in recent years. Attacks linked to social engineering such as voice phishing have become more popular due to the rise of artificial intelligence. Malware has also played a key part in cyber espionage since the creation of the internet, exploiting vulnerabilities in software of government or confidential information. A recent cyber attack using this method was carried out during the Covid 19 pandemic where actors from mainly Iran, China and Russia breached laboratories in the United Kingdom, United States, Japan and a few other countries. This was instantly addressed on the global political scale and reflects the threat to global security and rising world tensions cyber espionage can have.

Sabotage

Sabotage reflects a more desperate escalation of warfare compared to espionage which takes place even outside of wartime. Cyber attacks linked to sabotage mostly aim to completely disrupt or remove a piece of digital information, almost like how a bomb is used in war to handicap a target. In this sense, a sabotage cyber attack is truly the “bomb” of digital and cyber warfare. An example of sabotage in cyber warfare is a Distributed Denial of Service (DDos) attack on the Netherlands in early 2025 suspected to come from Russia. The motivation for the attack was the increasing support for Ukraine by setting aside up to 4 billion euros in funds for the next year. Not much is released about the nature of the attack; it is known that its effect was “minimal” due to the fast-responding efforts of the European Union's cyber security agency and the Dutch MIVD (Militaire inlichtingen en veiligheid). The attack taking place during an ongoing war reflects the nature and circumstances which a county has to be in to execute a cyberwarfare in the form of sabotage

Attacks on infrastructure

Infrastructure makes up a key part of a functioning and developing country. Infrastructure commonly targeted by cyber attacks can include power grids, power plants, water systems, medical systems and communication networks like phone lines or the internet. The latter of which is vital during times of war suggesting the incentive for a cyber attack on infrastructure. A recent example of

an attack on infrastructure was an attack on the United States healthcare system in 2024 suspected to originate from Russia. The repercussions of this attack were massive, leaving the healthcare system down for nearly a month. The preparators used a ransomware attack to effectively hold the healthcare system's data hostage until an unnegotiable price was paid. The American Hospital Association referred to the attack as "the most significant and consequential incident of its kind against the U.S. health care system in history.". Highlighting the rapid advancements of cyber attacks and their repercussions they can have infrastructure aiding global insecurity.

Propaganda

For centuries propaganda has been used to sway the opinions of populations often in a coercive manner and utilising social engineering tactics to better persuade an audience. As discussed previously, social engineering is a key aspect of cyber warfare and digital propaganda is one of the main applications of it. Cyber-propaganda as it is sometimes called, manifests itself in common day to day activities including news articles, social media sources suggest that cyber propaganda is a relatively new and developing concept having first been used in 2007. A major event in cyber propaganda was in 2014 where black hat hackers compromised data from the Democratic National Committee (DNC) which is responsible for promoting the Democratic party in the United States. The actors leaked parts of the stolen information to manipulate the population's opinion.

Attacks on Economies

Similarly to infrastructure, the economy plays a key role in a functioning country which makes it an attractive target for people seeking to commit a cyber attack. Attacks on an economy are often known to lead to increases in world tension, normally due to their high-profile nature, often targeting vital aspects of wartime economies like the stock market. Stable financial institutions like the stock market allows money to be transferred between investors and companies. A cyber sabotage attack on such an institution cripples the countries' ability to wage war. This type of cyber attack is done by halting transactions, since in the modern age transitions are all digital, they become more vulnerable to cyber attacks. Another example of cyber economic warfare are attempts to destabilize currencies which can lead to inflation. Finally, attacks on business are regarded as some of the most disruptive forms of warfare on economies as it can slow down production, disrupt supply chains and cause unemployment.

Major Parties Involved

Private Sector and local organisations

Businesses, although not national entities, play a key role in the economy of a country. Disrupting high profile business with a cyber attack can lead people to lose faith in the product which causes unemployment which can cause long term effects on a country. This is why private sectors often come up with their own form of cyber security organisations to combat data breaches. Such high-profile companies host large amounts of personal data. Examples include Microsoft, Apple, Google and Amazon. It is also important to note that cyber warfare is often conducted by individuals who are either funded by a government or just motivated out of pure nationalism or pride for their country to commit a cyber attack.

National organisations

Some national organisations have been mentioned previously in this report such as the MIVD in the Netherlands. National organisations against cyber crime deal with more serious cases of cyber warfare like attacks targeting government systems with the aim of stealing data from or impeding the process of the digital wings in the government. Some examples of national organisations tasked with cyber security are the Cybersecurity and Infrastructure Security Agency (CISA) in the United States or the National Cyber Security Centre (NCSC) in the United Kingdom.

International and worldwide organisations

International organisations for cyber security are often formed between political and economic alliances around the world and function similarly to national organisations. Some examples of such organisations are the European Union Agency for Cybersecurity (ENISA) or the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Worldwide organisations often vow to achieve larger goals summarised by this report, goals like promoting global security in a digital age. Some examples include The Global Forum on Cyber Expertise (GFCE) and International Watch and Warning Network (IWWN)

Timeline of Key Events

Date	Description of event
2004	The International Watch and Warning Network (IWWN) founded. Created to facilitate international collaboration on cyber threats
March 13th 2004	The European Union Agency for Cybersecurity. Focuses on cyber security in Europe
2007	First uses of cyber propaganda
May 14th 2008	NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) founded. Focuses on cyber security and warfare in NATO
January 1st 2012	The National Cybersecurity Centre was established. The UK's cyber security wing
2014	Major event in the development of cyber propaganda. Targeted attacks on the US democratic party possibly affected the election results.
April 2015	The Global Forum on Cyber Expertise (GFCE) founded. Aims to address the growing need for cyber capabilities internationally
November 16th 2018	The Cyber security and Infrastructure Security Agency (CISA) founded by the trump administration
January 6th 2020	The Global Forum for Cyber Expertise founded. Aims to create a cyber- secure world
2020-2021	Many cyber attacks take place in western countries like in the United Kingdom, United States, Japan during Covid research

UN involvement, Relevant Resolutions, Treaties and Events

- Combatting criminal misuse of information technologies, January 2001 (55/63)
- Combatting criminal misuse of information technologies, January 2002 (56/121)
- Creation of a global culture of cyber security, January 2003 (57/239)
- Creation of a global culture of cyber security and the protection of critical information infrastructure, January 2004 (58/199)
- Creation of a global culture of cyber security and taking a stock of national efforts to protect critical information infrastructure, March 2010 (64/211)

Previous Attempts to solve the Issue

Cyber literacy in schools

Cyber literacy refers to the ability to understand and use information and communication technologies (ICT). During the mid 2000s, education boards revealed that the average person did not know how to efficiently browse and use a computer. Because of this, mostly western schools took a new initiative to increase digital or cyber literacy. Such initiatives have continued until today and have become more extensive. As a result of this, digital literacy today is highest for people aged 30 and below as indicated by figure 1 that depicts “Digital Literacy and Financial Market Participation of Middle-Aged and Elderly Adults in China”.

Monitoring programs and agencies

As you are reading this, there are agencies around the world constantly searching for threats of cyber attacks. This has been the most effective way to prevent a cyber attack to date. The concept behind monitoring programs is to prevent the attack from happening before it even happens. Some such agencies include, as mentioned previously, the Cybersecurity and Infrastructure Security Agency (CISA) in the United States, the National Cyber Security Centre (NCSC) in the United Kingdom and the European Union Agency for Cybersecurity (ENISA). These agencies often work alongside other security agencies in the country. For example, the CISA in the United States works with the commonly known Federal Bureau of Investigation (FBI).

Possible Solutions

Cyber literacy

To reiterate, cyber literacy refers to the ability to understand and use information and communication technologies (ICT). These skills make a big difference when it comes to preventing cyber attacks. Often cyber attacks take place due to a country's or origin's inexperience in using and operating computers leading to gaps in their digital protection which could lead to a breach. Running courses for government officials or implementing digital awareness in school or university curriculum

could be ways to increase cyber literacy and prevent future cyber attacks and make the world a more secure place. Such a school course could include critical thinking against social engineering and phishing tactics that are used in cyber warfare. Although it has been shown as mentioned previously that the newer generations are already digitally literate (refer to figure 1) so the focus would be to teach the senior members of society which are more than often the ones working at high levels in most countries' administration and at high positions in businesses.

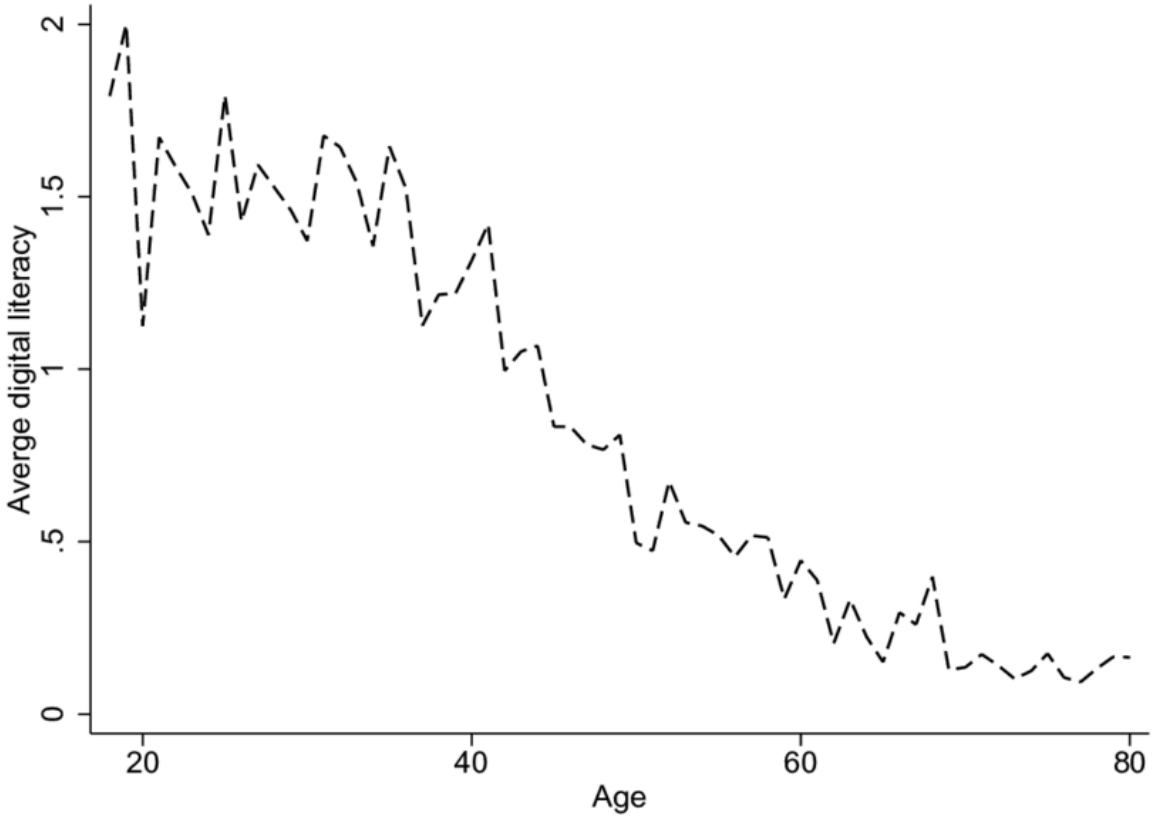

Figure 1: Digital Literacy and Financial Market Participation of Middle-Aged and Elderly Adults in China

Upgrading software

Computer systems in high-ranking sectors of government and business are often known to be running outdated software which presents an increased risk of cyber attack. The truth is that software should be replaced as fast as new methods in cyber warfare develop. Many countries that are considered to be more economically developed countries (MEDCs) have revealed that they have only recently modernised some government sectors from the era of magnetic storage and floppy

disks. Upgrading software may also include countries developing modern antivirus systems for their computers with important data or creating custom firewalls to prevent infiltration or a cyber attack.

Taking an analogue approach

Analogue is the opposite of digital. It may seem counterintuitive in a modernising digitalising world to reject progress, but sometimes not everything can change. The cloud is an example of a digital form of data storage that has become popular. The fact that it requires the internet and global networks to function implies that in some way or another it could be prone to cyber attacks. Reverting to an analogue form of data storage i.e. USB, Solid state drives, Hard drives and SD cards are more secure for companies and governments to store vital data safely. This doesn't however prevent the risk of a ransomware attack or any sort of viruses

Bibliography

"10 Easy Ways to Protect Yourself from Cyber Attacks." Victoria University, Australia, 2022, www.vu.edu.au/about-vu/news-events/study-space/10-easy-ways-to-protect-yourself-from-cyber-attacks.

"10 Ways to Prevent Cyber Attacks." Leaf, 2023, leaf-it.com/10-ways-prevent-cyber-attacks/.

Baker, Kurt. "What Is Cyber Espionage? | CrowdStrikee." Crowdstrike.com, 16 Jan. 2025, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.

Candan, Bahadir. "Top 5 Critical Infrastructure Cyberattacks." Www.anapaya.net, 23 Feb. 2023, www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks.

"Common Cyber Attacks: Reducing the Impact." Www.ncsc.gov.uk, www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact.

"Cyber Propaganda 101 | Trend Micro (NL)." Trendmicro.com, 10 Mar. 2017, www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/cyber-propaganda-101. Accessed 30 June 2025.

"Cyberwarfare, N. Meanings, Etymology and More | Oxford English Dictionary." Oed.com, 2023, www.oed.com/dictionary/cyberwarfare_n?tab=factsheet#99138378819, https://doi.org/10.1093//OED//3321304927. Accessed 30 June 2025.

D'Souza, Deborah. "How the Modern Stock Market Is Affected by War." Investopedia, 23 Sept. 2022, www.investopedia.com/solving-the-war-puzzle-4780889.

Fortinet. "What Is Cyber Warfare?" Fortinet, 2024, www.fortinet.com/resources/cyberglossary/cyber-warfare.

Imperva. "What Is Cyber Warfare | Types, Examples & Mitigation | Imperva." Learning Center, 2022, www.imperva.com/learn/application-security/cyber-warfare/.

Kaspersky. "Wat Is Social Engineering? | Definitie." /, 10 May 2018, www.kaspersky.nl/resource-center/definitions/what-is-social-engineering.

Kenton, Will. "War Economy." Investopedia, 2019, www.investopedia.com/terms/w/war-economy.asp.

Lan, Sai. "Digital Literacy and Financial Market Participation of Middle-Aged and Elderly Adults in China," *Researchgate*, Oct. 2021.

Martin, Alexander. "Russia Attempting Cyber Sabotage Attacks against Dutch Critical Infrastructure." Therecord.media, The Record, 22 Apr. 2025, therecord.media/dutch-mivd-report-russian-cyber-sabotage.

"Militaire Inlichtingen En Veiligheid (MIVD)." Defensie.nl, 2025, www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid. Accessed 30 June 2025.

"What Is Cyber Espionage | VMware Glossary." Broadcom.com, 2024, www.broadcom.com/topics/cyber-espionage.

Appendix or Appendices

www.fortinet.com/resources/cyberglossary/cyber-warfare

This is a useful link the summaries the report quite well

https://www.itu.int/en/action/cybersecurity/pages/un-resolutions.aspx

This has all the past resolutions on cyber security