# OSJMUN
# Disarmament Committee

Issue:
Threats to International Peace and Security Caused by Cyber Warfare

**Forum: Disarmament Committee**
**Issue: Threats to International Peace and Security Caused by Cyber Warfare**
**Student Officer: Esin Dinçer**

## Introduction

As warfare evolves, new methods of attack are being developed and utilized, with cyber warfare being a prominent weapon capable of high levels of damage. Cyber warfare has become a common tool to be used by various organizations with malicious intentions to attack their targets, with such attacks growing in quantity and complexity with each passing year. Nation states such as the United States, China, and North Korea are the most prominent in the field of cyber warfare, but more nations are quickly developing such capabilities for themselves. To counter the threat of cyber warfare and cyber-attacks, both the public and private sectors have invested heavily in defending their networks, but they still cannot protect against every attack. Therefore, more measures are needed to regulate actions that can be undertaken by nation states and studier defenses against outside attacks.

Our modern society demands a degree of connectivity between citizens, businesses, financial institutions and governments that must cross political and cultural boundaries. Digital technology provides this connectivity and gives its users many valuable benefits. But at the same time, it provides a rich environment for criminal activity, ranging from vandalism to stolen identity and to theft of classified government information.
Computers, computer networks and the Internet were created to improve creativity among people, store information, transfer governmental information and share information. The creation of a digitized method may have pushed mankind into the 21st century but it did the same thing to criminals. Hackers want to reach the information that we have .The more difficult it becomes to find; the more eager they become to solve the problem

Cyberspace, a domain not created by nature but by human beings, has emerged to provide tremendous benefits, but also to present new risks. Recently, cyber security has become a national issue. Driven

predominantly by national security concerns, democracies have formulated national cyber strategies.

Consistent definitions are essential. Cyberspace refers to inter-connected information technology infrastructures comprising computers, computer-embedded systems, telecommunication networks, the world wide web and the internet, including the information transmitted and processed within these systems. The public internet is only one part of cyberspace. Other parts include mission-specific systems that vary widely in size and complexity and control the function of various obscure processes; these control functions gradually become computerized. The term "cyber," derived from Greek, refers to the control element.

## Key Terms

**Cyberwarfare:** the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

**Vandalism:** Action involving deliberate destruction of or damage to public or private property.

**Hacktivist:** A person who gains unauthorized access to computer files or networks in order to gain social or political ends.

**Network:** A group or system of interconnected people or things.

**Cyberspace:** The notional environment in which communication over computer networks occurs.

**Property:** A thing or things belonging to someone; possessions collectively.

## Risks of Cyber Attacks Between Governments

In recent months, there is a growing tension between western countries and Russia, highlighting the growing risk of cyber-attacks by nation states and their allies.

Russia has been accused of waging a digital war against the west. It has allegedly interfered with elections in the US and Europe, it has been linked to a global malware outbreak, and has been accused of targeting the IT systems of critical infrastructure and services.

The UK is not alone in accusing Russia of cyber activities. Germany says Russia attacked its Foreign Ministry while the US recently blamed Russia for cyber attacks on its energy grid. UK and US officials believe that Russia has been probing networks in preparation for potential acts of sabotage, such as taking down parts of the electricity grid. In February, the UK, US, and Australian governments said Russia was behind the NotPetya malware attack, which initially targeted Ukraine in June 2018 but quickly spread around the globe.

The world observes the emergence of hybrid warfare whereby foreign rivals are actively seeking to disrupt economic capacity, targeting the business sector, public services and critical infrastructure.
State sponsored cyber attacks are now one of the most serious risks facing cooperates today, and yet this is one of the most underappreciated risks at board or C-suite level. Most companies do not realize that they are the targets of foreign intelligence services looking to steal intellectual property, ideas and technology, or just to disrupt business and the wider economy.

Russia is not the only country using its cyber capabilities to further its interests. Hacking groups linked to other nation states, most notably North Korea, Iran and China, are also known to be actively deploying sophisticated cyber capabilities.

Nation states are thought to be behind a number of cyber attacks in recent years against banks, energy companies, government agencies and suppliers of critical services and infrastructure. Attacks can be for a wide range of purposes, including the theft of intellectual property, trade secrets or personal data, as well as to cause disruption or physical damage.
According to a report by Crowd Strike China ,they have targeted western commercial interests and government agencies as they seek information and intelligence that may provide military, diplomatic or commercial advantage. In the case of North Korea, nation state-linked hackers are said

to be behind extortion attacks and cyber heists, while the country was blamed for last year's global ransomware attack, WannaCry.
Iran's cyber activities have largely targeted entities in the Middle East, notably the Shamoon malware destructive attacks against Saudi Arabia in 2017. The US and UK recently condemned Iran for cyber-attacks against western universities.

## Timeline of Cyber War Attacks

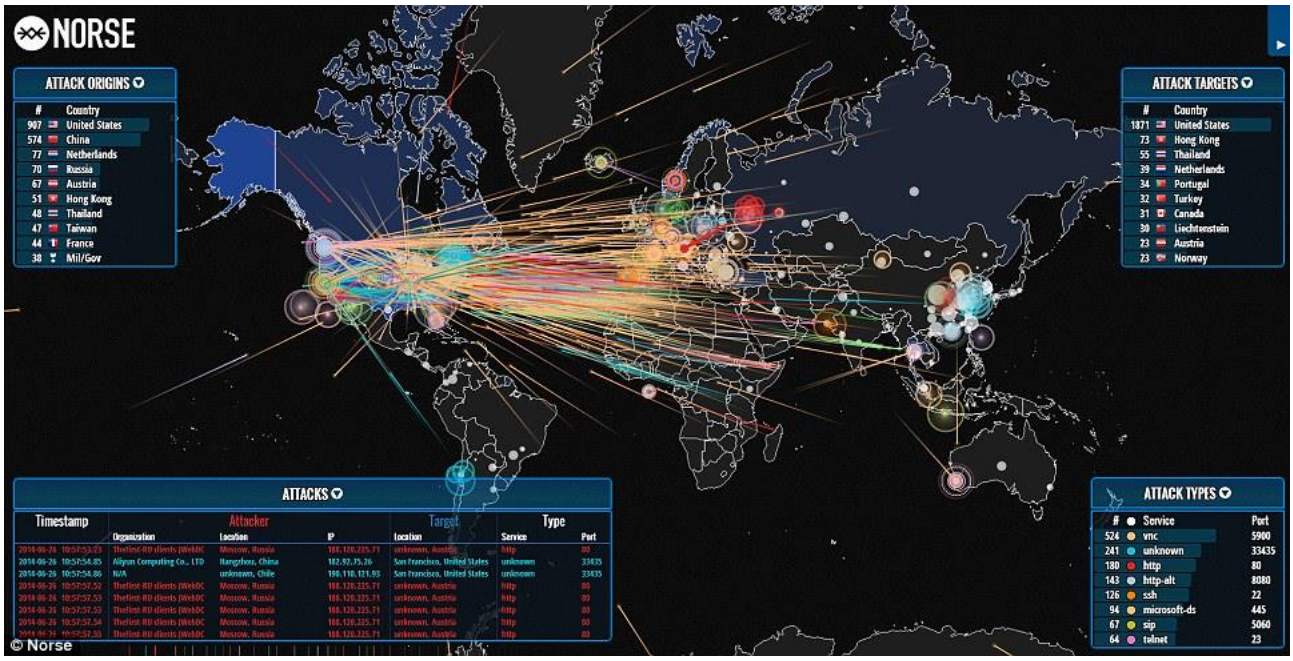
**2007:** Israel is suspected to have used computer attacks to neutralize parts of Syria's air defences in advance of an airstrike against the Arab country.

**2008:** A digital breech of unknown origin brought havoc on the Republic of Georgia. At the same time Russian troops launched operations in the Caucuses. Is it a coincidence? The year before a computer attack on Estonia briefly disrupted both the government and the national media. The incident coincided with a controversial plan by Tallinn to relocate a Soviet era war memorial known as The Bronze Soldier. The hack was traced to Russian government computers.

**2010:** In September, Iran's nuclear enrichment facility at Natanz fell prey to what is believed to have been a joint U.S. and Israeli cyber attack, dubbed Operation Olympic Games. The mission involved the depositing of a computer virus known as Stuxnet into the site via an infected USB stick. The malicious code reportedly crippled software and hardware for many of the site's centrifuges disrupting Tehran's nuclear bomb program.

**2011:** Unknown assailants briefly locked the USAF out of its own drone fleet at Creech AFB in Nevada. Later that same year, Iran reportedly severed the GPS link with an American Predator operating over Afghanistan, gained control of the aircraft and brought it down safely onto an airstrip inside their borders.

**2012:** *The New York Times* reported that a number of military and corporate computer networks in the United States were attacked by China's cyber warfare division, Unit 61398.




**2016:** The foiling of a North Korean attack on 140,000 computers in South Korea made headlines just a few years ago. Seoul reported that hackers in Pyongyang dropped malicious code into 160 civilian and government systems in preparation for a massive surprise cyber attack. And this wasn't a first for the so called Hermit Kingdom. In late 2014, Kim Jog-un supposedly ordered a hack against Sony Pictures for its release of the the comedy *The Interview*, which famously spoofed the North Korean dictator.

## Possible Precautions for Cyber Attacks

When it comes to protect a nation from cyber attacks, we can see some basic precautions. In many cases, a government itself makes cybercrime possible. One of the most common and critical mistakes governments make is focusing solely on the technical aspect of cyber security. For example, let's say a government spends thousands of dollars on network perimeter security, investing in the best firewalls, intrusion detection systems and so on…
After such a large investment, that government would expect to see results; however, instead, a security breach happens. Why? Because the government has neglected to provide its citizens with proper training.

This is the point that we can see the importance of public awareness. Transferring the general information and raising public knowledge is very important in controlling the issue of cyber attacks. Cyber wars are not only caused by international conflicts, but also can be a perplexed version of cyber attacks happening in national boundaries.

*Create International Guidelines or Framework Regarding Cyberwarfare*

Most existing laws simply mandate that organizations must protect themselves from cyber attacks. There needs to be measures to protect innocent civilians from the machinations of malicious institutions, and only the United Nations has the authority to create such overarching international laws. These laws can hold nation states liable to any damages they cause to another country and hold them responsible for their actions to deter future cyber attacks. Against other organizations, these laws would not deter them from attacking, but can be used to punish them for their actions, like the Geneva Conventions on the rules of war.

*Enforce Standardized Cyber security Regulations*

One of the problems facing cyber security is that not everyone has the same levels of security, allowing cyber attacks to target the ones more vulnerable to gain a foothold and continue their attack on more secure targets. By ensuring that as many people have the most up to date protective software, thorough methods such as having a governmental body audit company networks and holding companies legally responsible for failing to follow the regulations, it can hamper most of the cyberattacks and prevent serious breaches of data. In addition, by informing the people on what threats they face, they can take more preventive actions themselves and refrain from enacting risky decisions that could compromise their network.

## **Chair's Notes:**

Fellow delegates, as we all know, in the 21st century, the virtual world is as big as the real world. Bank accounts, chats, connections between politicians and so on…

These are just a few very important things that internet allows us to arrange online. Therefore the importance of cyber security is undeniable. With this topic, we are going to debate about the threats of cyber attacks, how important the cyber world is and the possible solutions. I want all of you to be creative and productive. These 2 days are going to be very efficient and you are going to have the opportunity of sharing your important ideas with others.

Please be aware of the fact that you are going to represent countries which have strategic importance on that issue. All of the countries can add something and change the course of the resolution. While you are doing this, please do not forget to learn new things and have fun. This is going to be an unforgettable experience for all of us!

## **Bibliography**


"Arms Control Today." Nonproliferation Benefits of India Deal Remain Elusive Arms Control Association,www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-onCybersecurity

Breene, Keith. "Who Are the Cyberwar Superpowers?" World Economic Forum, www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

"Cyber Warfare Is Growing. We Need Rules to Protect Ourselves." Futurism, Futurism, 20 Feb. 2018, futurism.com/cyber-warfare-rules-protect-ourselves/.

"Hack Attacks - A Brief History of Cyberwarfare." MilitaryHistoryNow.com, 22 December 2016, militaryhistorynow.com/2016/12/21/surprise-e-ttack-a-short-history-of-cyberwarfare/.