Committee: Special Conference on Cyber Governance

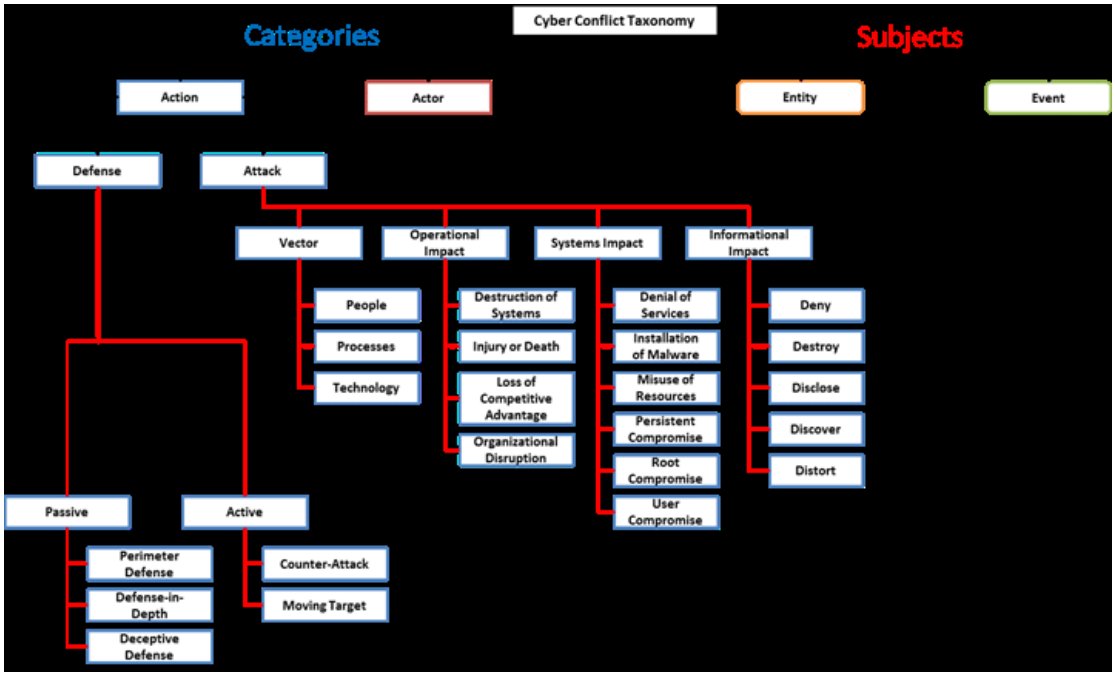
Issue: State response in addressing new challenges in cyber conflicts

Student Officer: Mike Papakonstantinou

Position: Deputy President

INTRODUCTION

In the past years, technology reached its peak and exhibited constant improvements. However, despite the fact that there have been massive advantages, there have also been massive consequences and disadvantages for international cyber security. Cyber conflict has become a source of worry for many nations' policies and governments, due to the fact that it grows exponentially and it has become a major threat for the citizens' private safety and prosperity. Cyber conflict outbreak is responsible for various crises around the globe, which had serious results and created a great concern. Nations have given many efforts to solve the issue in a satisfactory level, but it seems like the problem is getting larger and more fatal every day.



The United Nations have struggled to find an adequate solution to this immense issue, or even to restrain its consequences. Even with the measures that have been proposed, the problem seems to be getting larger every day. This, alongside with the consequences in the

digital world and the continuous threat for citizens' safety in the Net, are some of the reasons that a final solution must be found.

DEFINITION OF KEY TERMS

CYBER

Word related to or characteristic of the culture of computers, information technology, and virtual reality.

CONFLICT

Competitive or opposing action of incompatibles: antagonistic state or action as of divergent ideas, interests, or persons (Merriam-Webster)

CYBERSPACE

The online world of computer networks and especially the Internet (Merriam-Webster)

SOFTWARE

Used or associated with and usually contrasted with hardware such as programs for a computer

MALWARE

Malware is any software intentionally designed to cause damage to a computer, server, and client or computer network.

BITCOIN

A type of digital currency in which a record of transactions is maintained and new units of currency are generated by the computational solution of mathematical problems, and which operates independently of a central bank.

CYBER SECURITY

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. (Kaspersky Lab)

SERVER

A computer or computer program which manages access to a centralized resource or service in a network.

IT INFRASTRUCTURES

"IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities." (Techopedia)

BACKGROUND INFORMATION

New challenges in cyber conflict

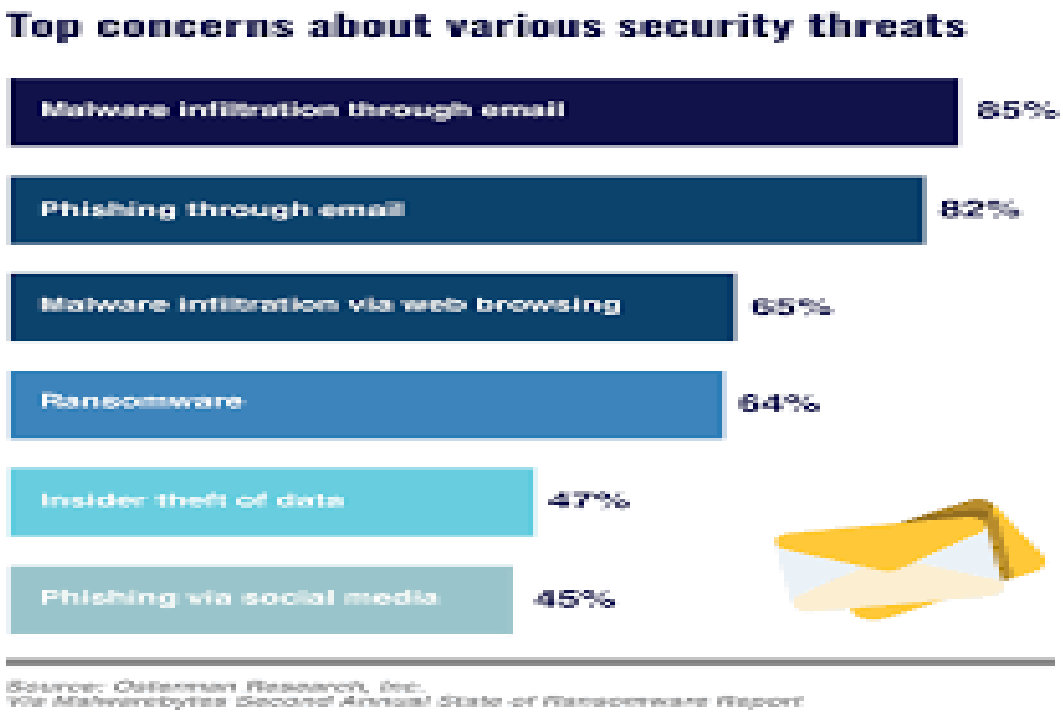
The issue calls the states represented in our committee to respond to new challenges in cyber conflict. But what are these new challenges anyway? The United Nations Institute for Disarmament Research (UNIDIR) alongside with the Institute of Peace Research and Security Policy at the University of Hamburg and Freie Universität Berlin, held a two-day conference regarding challenges in cyber security on 13-14 December 2011 in the Federal Foreign Office in Berlin. The conference report presents some interesting facts, as it mentions risks in cyber security as well as recommended strategies in state response. Various challenges are also underlined in the report.

The conference had a background of the potential impact of the emerging threat of cyberattacks, clearly stating that the costs and the unanswered questions regarding security can be fatal for any state, both for its government as for its citizens.

These challenges were addressed in six Track sessions. The overview of the conference had 6 pillars, to develop joint approaches to keep the Internet as global commons, the understanding of global strategies on cyber security, the emerging economic and social risks etc.

The outcome must become food for thought for any State in the planet, as it must be used for guidance in the upcoming regulation and policy changes. Specifically, the measures that are proposed will be referred to the Possible Solutions section of the study guide.

Although cyber-attacks have been spreading in the past few years and can be described as a relatively new phenomenon, they have been destructive for several private companies, worldwide organizations, or even entire nations. The term 'cyberspace' was first used in the 1960s, but it had nothing to do with what we refer to as 'cyberspace' today.



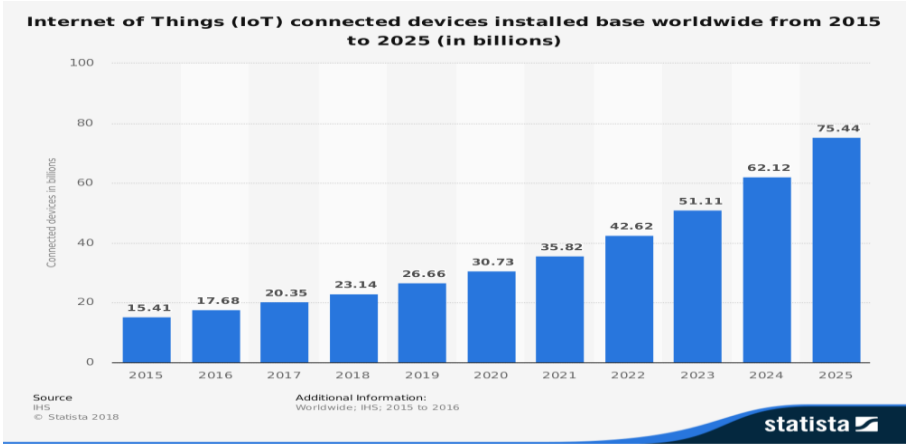
The first officially recorded cyber-attack occurred back in November 1988 from Robert Tappan Morris, son of the famous cryptographer Robert Morris Sr. The interesting fact about this attack is that it happened accidentally. Morris created a program that would keep count of how many computers have access to what is known today as 'cyberspace'. He did that by asking each machine to send back a signal to a central server and that server would keep count of the signals sent. The program worked better than expected. In fact, it worked too

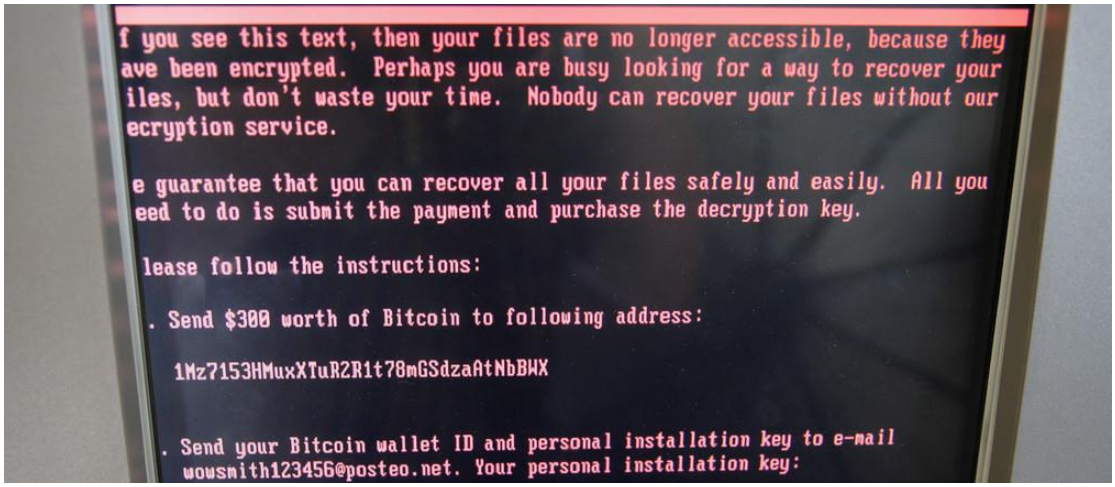
well. The program was clogging up major sections of the cyberspace and Morris was unable to stop the problem due to its scale. These kind of attacks are called ‘distributed denial of service’, which means that multiple devices are sending multiple signals or information to a specific address which is later overloaded and stops working.

In simple terms, cyberspace is the worldwide network that connects a vast amount of electronic devices that have access to the Internet. Here is a chart of the number of electronic devices that the world will have by 2025.

Cyber conflict can and will soon be a strategic problem for most nation states, especially for the MEDCs and the countries that technology and the Internet are widely spread. The consequences of cyber-attacks can be sweeping. They can vary from social to economical to even political and can compromise a whole nation in just a few minutes. Bank systems can collapse, social media platforms can overload, communications can be corrupted and in a glance of time a nation can find its self in an emergency situation. This is the reason why cyber activity and cyber governance is such a delicate issue.

Many nations have already proceeded in cyber conflicts against organizations or other countries.





Here is an example of a cyber-attack in a private server. The intruder managed to encrypt the files of the server and now demands from the user to pay an amount of Bit coin currency in order to make the files accessible. (Image: REUTERS/Valentyn Ogirenko)

The spreading of national cyber attacks

The spread of national cyber-attacks especially on the private sector is massive. Several attacks that paralyzed national security systems in various nations have been recorded in the past 3 to 4 years. Here are some examples that will help you see the issue from a greater perspective:

Ukraine, Russia, June 27, 2017

The damage of the specific wave of powerful cyber-attacks hit the whole European continent but it was greater in these two countries. The companies that were severely affected were Russian oil giant, a Danish shipping company as well as Ukrainian government ministries, which were 'brought on a standstill in a wave of ransom demands' as Washington post mentions. People's lives were also in danger as major systems at the site of Chernobyl shut down forcing scientists to monitor radiation levels manually. This cyber-attack created political suspicions between Ukraine and Russia, countries that already suffer from a diplomatically crisis due to the issue of Crimea.

New Jersey, November 2017

New-Jersey based pharmaceutical company Merck fell victim of a major cyber-attack in November 2017. Still it wasn't the only private company that was compromised from the specific attack. As Merck mentioned on Twitter, 'the company's computer network was

compromised today as part of a global hack'. Cyber researchers reportedly mention that the virus was linked to a malware called Petya, which used a National Security Agency exploit, which was leaked by hackers and became accessible through the Internet.

Saudi Arabia, November 2016

An aggressive computer virus compromised Saudi Arabia's aviation agency on November 2016. The attack targeted high-profile government targets and officials. The attack was triggered from a source outside the country and most likely used a kind of malware that is characterized as a data-clearing malware.

What the global community has learned from these cyber-attacks is that every single server, whether we are talking about public or private sector, is compromised when it has access to cyberspace. It does not matter if it is in Europe, Asia or the Americas. If the proper security measures are not taken, things will get even worse than they are, and these kinds of attacks will spread even faster.

To detect cyber-attacks several maps have been created. One of the most reliable is Threatcloud. Threatcloud records the source of the attack and its target. It is an available free and non-governmental service, accessible from any computer with access to the Internet.

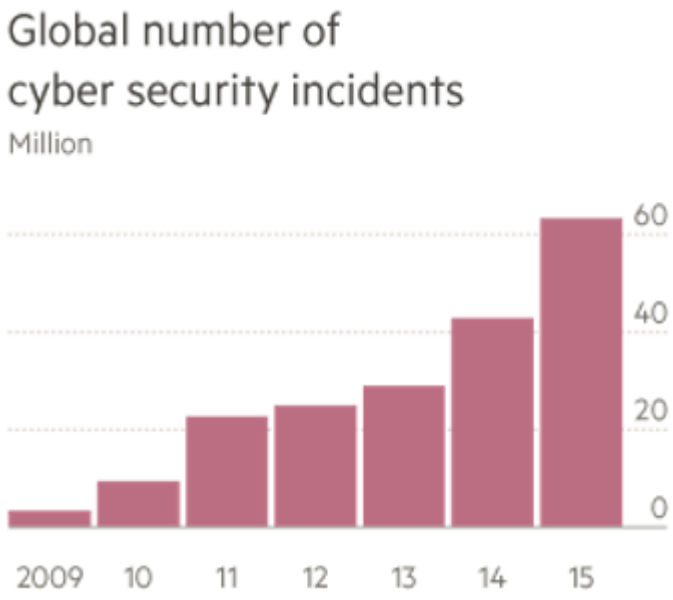


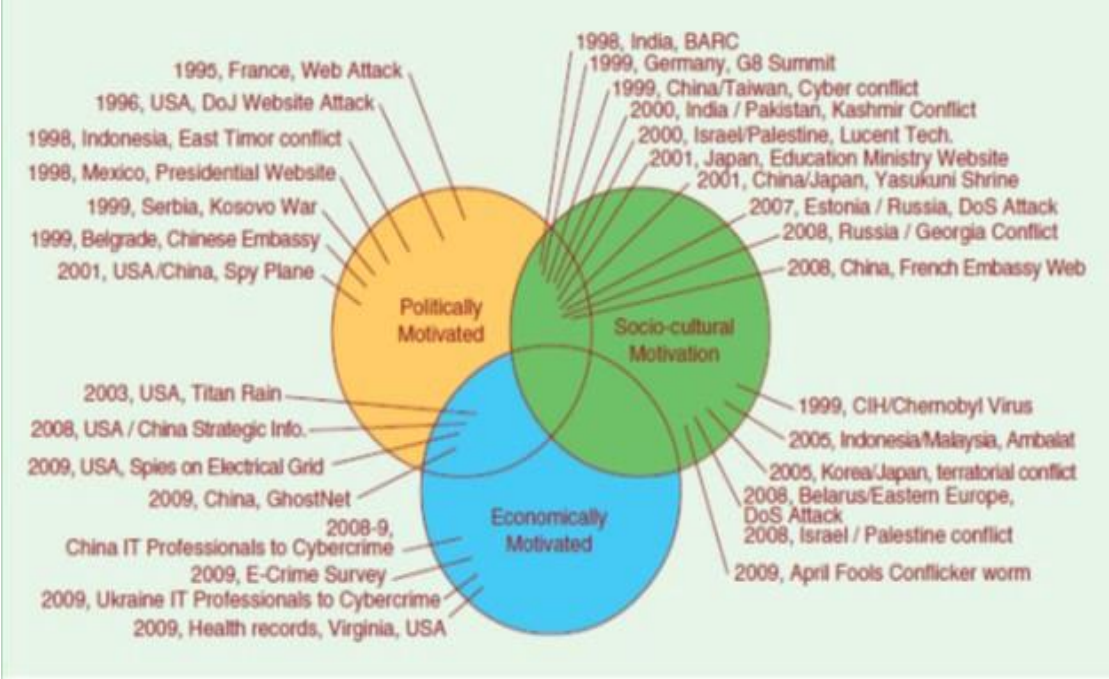
Image: Financial Times, Check Point, PwC

There is still not a universal definition of cyber warfare in existence. Even the agreement on how the word is spelled has proven elusive. For most people, this could be a sign of cyber warfare being irrelevant. However, cyber warfare is a very delicate matter. With over 27 million cyber-attacks happening every day, a cyber-war could occur at any time. So it is crucial to analyze what cyber warfare is.

Cyber warfare refers to the actions by a nation or an organization to attack and damage another nation's network's available information through viruses or denial-of-service attacks. Many cyber weapons are mostly based on software vulnerabilities that can be found on networks that drive health care, manufacturing, power generation and distribution, and transportation among other national and private sectors.

On April 2018, the United Kingdom and the United States of America had an unprecedented joint statement blaming Russian Federation for several cyber-attacks on businesses and consumers. National Cyber Security Centre and the FBI were forced to warn citizens and companies concerning Russia's actions that exploit network infrastructure devices around the globe. It is known that Russia is probably the most successful nations when it comes to state sponsored attacks. On the other hand, several nations including China, North Korea and Iran reportedly own cyber arsenals to threaten western nations. In general, Russian Federation and the Kremlin have been accused several times for actions that might indicate cyber warfare among three nations, Russia, US and the United Kingdom.

Several facts suggest that a single cyber-attack managed to influence the US presidential elections in 2016. However, a full blown cyber-attack is something else. For example, it could mean the complete shutdown of a Ukrainian power unit, two times or the wipeout of bank accounts and data centers due to a malware that caused financial panic in South Korea on 2013. Cyber warriors are established mostly by the United States, who conduct intelligence gathering operations and support military missions.



MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

Israel

Israel has its part in cyber-attack response, however resulting in the loss of a human life. On May 2019, Israel Defense Forces targeted and destroyed a building associated with an on-going cyber-attack. It is also considered one of the 5 cyber powers.

United States of America

United States of America has played its part in cyber warfare, both when it comes to its national engagement upon the issue, as well as in their cyber warfare alliances. In general, the US has been found in the middle of the action in several cases of cyber-attacks. This is the reason that the States have taken direct political action regarding cyberspace security. President Barack Obama and his administration in 2012 started with the PPD-20 (Presidential Policy Directive 20). This required a complex and lengthy interagency legal process before approval of any offensive cyber operation. President Donald Trump decided to rescind PPD and create a new policy that merges the Defense Department and the intelligence agencies. On September 2018, the White House and President Trump delivered the National Cyber Strategy, a document of 15 pages available online which describes in detail the position of the States towards cyber security of the nation. Notable facts are the

cyber alliances with the UK as well as its position against cyber-sponsored Russian cyber-attacks.

Russian Federation

Russian Federation is well known for its denial-of-service cyber-attacks as well as their connection with several cyber warfare acts towards nations such as Estonia, France, Germany, Georgia, Kyrgyzstan, Poland, Ukraine, Venezuela and the influence in the 2014 Ukrainian presidential elections, the Brexit referendum and the United States of America. These attacks were mostly conducted for election or campaign influence such as the case of Macron's presidential campaign where 20000 emails were leaked by a Russian-associated hacker group, APT28, or for diplomatic issues such as the case of Estonia for the Cold War memorial.

People's Republic of China

China is considered one of the 5 superpowers of cyber warfare alongside United States, Russia, Israel and the United Kingdom. In the last 2 years, news stories about China and cyber-attacks have been adding up and it seems like the nation has high intentions for cyber warfare. Chinese Military Strategy describes the primary objectives of cyber capabilities to include 'cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation'.

Germany

Germany is possibly the country with the most developed cyber security policy in Europe. Their policy is called "Netzpolitik", which translated from German means the policy of the Internet. This policy aims to keep the Internet as a free commons for all people to express ideas and opinions, but at the same time secure the safety of its users. Many experts of the field strongly support this policy as a lesson for other nations to perfect their strategy against cyber policy.

NATO

The member nations of NATO have been very active in a short time period when it comes to cyber security. In 2014, the Allies made cyber defense part of collective defense, reportedly declaring cyber-attacks as invocations of the collective defense that Article 5 suggests. Later

on in 2016 the Allies recognized cyberspace as a domain of military operations and prioritized the enhancement of cyber defenses of national networks and infrastructures. Most recently in 2018, the Allies agreed on the integration of sovereign cyber effects into operations and missions as well as to stand up the Initial Cyberspace Operations Centre.

National Security Agency (NSA)

The National Security Agency is a national-level intelligence agency of the US Department of Defense. It is responsible for global network monitoring as well as for information gathering and processing. NSA has played a big role in cyber warfare between the States, the United Kingdom and Russia. It owns encryption systems, software backdoors and several employees of the agency have participated in hacking operations of counter attack.

The SANS Institute

The SANS Institute is the most trusted and the largest source of information security and security certification in the planet. It also operates the Internet's early warning system, the Internet Storm Center.

TIMELINE OF EVENTS

October 24, 1945	The United Nations are formed after a catastrophic World War II.
1960s	The term 'cyberspace' is used for the first time.
November 1988	The first recorded cyber-attack occurs by Robert Morris.
1993	Checkpoint, the company that created Threatcloud, is founded by Rahmat Gann in Israel.
December 2011	The Conference on Challenges of Cyber Security is held in Germany.

2012	The PPD—20 is formed by Obama's administration.
2013	The cyber-attack that caused financial crisis in South Korea happens.
2016	The US presidential elections are influenced by Russian hackers.
November 2016	Saudi Arabia's aviation agency falls victim to a malware cyber-attack.
June 2017	A cyber-attack that spreads across Europe pledges Ukraine's government, bank system and the Chernobyl area.
November 2017	In New Jersey, pharmaceutical giant Merck falls victim of a global hack causing production to a temporary halt.
April 2018	UK and US have a joint statement against Russia regarding cyber-warfare.
September 2018	The National Cyber Strategy is formed by the White House and Trump's administration.
May 2019	The first human life is lost due to cyber warfare.
2025	It is estimated that over 75 billion devices will have access to cyberspace by that time.

UN INVOLVEMENT AND PREVIOUS RESOLUTIONS

Resolutions 55/63 (January '01) and 56/121 (January'02): The measures that these resolutions suggest are combating the criminal misuse of information technologies.
Resolution 57/239 (January '03): The measures that this resolution proposes suggest the creation of a global culture of cyber security.
Resolution 58/199 (January '04): The measures that the resolution proposes suggest the protection of critical information infrastructures and the creation of a global culture of cyber security.
Resolution 64/211 (March '10): The resolution proposes the usage of national stock to protect critical information infrastructures.

The UN Secretary General Antonio Gutierrez often urges for global rules on cyber security in order to minimize the impact of electronic warfare. He did so in one of his most recent speeches when he received his honoris causa degree in University of Lisbon on February 2018. However, UN involvement on cyber security does not go further than the resolutions above despite the urge from the Secretary General. In fact, the last resolution of the Security Council was formed on 2010 and that is a long time ago compared to the rapid development of the issue.

POSSIBLE SOLUTIONS

There are plenty of possible solutions that can be proposed in order to tackle the threat of cyber conflict and cyber warfare through efficient state response. Firstly, all states must be willing to retain the freedom that is contained with the help of the Internet. With this measure, we will be able to avoid protests of hackers through cyber attacks. Secondly, we must make sure that the worldwide agreements regarding cyber security are implemented correctly in every nation. Internet prosperity and unnecessary regulations that rescript the free use of cyberspace should be restricted. Every nation is obliged to follow the international regulations, not just for cyber security but for every issue. Third of all, the private sector and global businesses must make sure that they are not compromised from cyber attacks, that can cause massive economic crisis throughout the globe, if we are talking about a bank or a private business that has departments all around the world.

Another measure that can be proposed is a wider frame of legal regulations, that will idealy include international cooperation with states, governmental organizations, as well as NGOs for the establishment of rules to achieve the adequate behavior from Member States. Last but definitely not least, the issue of cyber militarization must be directly addressed from the Member States. Multiple nations have already begun cyber militarization programs and conversations must take place in order for this issue to not get out of hand any time soon.

Of course in any of you delegates have any other solutions to propose through your own research we will be glad to evaluate them in the upcoming conference. However, it is very important to take into high consideration all the facts you have in the study guide.

BIBLIOGRAPHY

Sciarrone, Marie O'Neill, Cyber Warfare: The New Front, https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html

International Association for Political Science Students, Cyber conflict: Addressing new challenges in cyber space and state response in the age of uncertainty, https://iapss.org/2017/09/07/cyber-conflict/

NATO Review, NATO's role in cyberspace, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

Wikipedia, Cyber warfare, https://en.wikipedia.org/wiki/Cyberwarfare

Freeze, Di. "List of Cyber security Associations and Organizations." *Cybercrime Magazine*, 19 Apr. 2018, cybersecurityventures.com/cyber security-associations/.

Kaspersky.com, www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

"Malware." *Wikipedia*, Wikimedia Foundation, 13 June 2019, en.wikipedia.org/wiki/Malware.

Khalip, Andrei. "U.N. Chief Urges Global Rules for Cyber Warfare." *Reuters*, Thomson Reuters, 19 Feb. 2018, www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

UN Resolutions, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

Jinghua, Lyu. "What Are China's Cyber Capabilities and Intentions?" *Carnegie Endowment for International Peace*, carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

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

Conference Report: "Challenges in Cyber Security: Risks, Strategies and Confidence-Building" http://www.unidir.org/files/medias/pdfs/conference-report-eng-0-373.pdf