Developing Counter-Measures against Cyber Warfare

Committee Guide

First Committee of the General Assembly

OLMUN 2018
18th International Session

Table of Contents

Personal Introduction

Hello everyone!
I am Christopher and I am honoured to welcome you to the GA1st committee!
I am 23, German-British and doing a master's degree in Physics at the University of Münster, where I recently also started doing research on quantum technologies as a scientific assistant. I did my Abitur at Herbartgymnasium Oldenburg and my bachelor's in Göttingen.
I love learning how the world works and I like my life to be diverse. I study Chinese, play Go, and Squash. Recently I started attending the local debate club. Whenever I have nothing to do I like to go to random lectures.
Above all, I like making friends. That's one of many good qualities of MUNs. This is my 9th conference. I have attended 4 high-school MUNs during 2011-2013 and 4 university MUNs during 2017-2018. This is my first conference as a chair. Furthermore, I'm doing lots of work as part of Münster's prestigious MUIMUN organizing team.
My memories of great OLMUN conferences motivated me to restart participating in MUNs and I'm very glad I did. MUNs are terrific fun, whenever one is brave enough to engage heavily in the process. If anyone would like advice on anything, please don't be afraid of approaching me! I am looking forward to a great conference with my co-chairs and all of you!

Dear delegates,
My name is Sören Wehrheim and I am pleased to welcome you to the GA First Committee at OLMUN 2018.
I am 23 years old and study computer science at the University of Paderborn in Germany, but I grew up in Oldenburg. OLMUN was my first MUN conference back in school, and I still come back every year to contribute in one way or another. Additionally, I have participated in over 50 MUN conferences on a university level, mostly as a delegate. For me, MUN offers a thrilling combination of my main interests: International politics and relations, excessive travel, and getting to know new people from all over the World.
Whether it is your first time as a delegate or you already have participated in another MUN before – my co-chairs and I will work hard to ensure that you will have the best possible experience. I am looking forward to meeting all of you!

Dear delegates of the GA 1st,
My name is Alexandra Wolff and I am very happy to welcome you to the GA First Committee at 2018's OLMUN. I am currently 16 years old and finishing 11th grade at the Cäcilienschule Oldenburg. Some of my hobbies include drawing and theatre, but also reading and politics. I am very new to OLMUN and MUN in general, having participated as a Delegate last year for the first time, an opportunity which I took to improve my public speaking skills and meet many new people, some of which even joined the OLMUN Inner Circle with me this year. I sincerely hope that OLMUN will be the fantastic experience to you that it was to me, and that, even as a first-time Delegate, you will be unafraid to contribute as well as enrich the discussion and just have fun.
Let's all enjoy a wonderful week together!

1. General Introduction

Honourable delegates of the General Assembly First Committee,
we are glad to welcome you to OLMUN 2018 and the city of Oldenburg! During the days of the conference, you will experience international diplomacy by taking the roles of diplomatic representatives of your assigned country. You will hold speeches, negotiate with your fellow participants, and work towards a solution for the issue at hand.
As OLMUN is a conference that caters to beginners, all proceedings will be thoroughly explained during committee session. However, we advise you to read the Rules of Procedure before the conference, which can be found on the OLMUN website. In order to represent your country accurately, you also need to be informed about the topic of the committee and your country's position.
This guide is supposed to give you a general overview of the committee and topic, and help you get started with your preparation. However, you are very much encouraged to do additional research. To represent a country accurately, it is important to have some basic knowledge about its history, geography, culture, political structure and relationships with other countries. When it comes to the topic, please look into the actions and commitments your country has made on a national and international level.
It is important to remember that your personal opinion on issues might deviate significantly from your country's position. For the sake of the debate it is necessary that you stick to your country's policy, even if you disagree with it.
Before the conference, you will be asked to prepare a position paper, which is a short summary of your country's position. More information about that will be provided closer to the conference.

2. Introduction to the General Assembly First Committee

The First Committee of the General Assembly (GA 1st) is one of the main committees of the General Assembly. It is known as the "Disarmament and International Security" committee, and deals with disarmament, threats to peace and global challenges. Its decisions are not legally binding, but represent a strong self-commitment of the international community. Resolutions passed by the First Committee are forwarded to the plenary sessions of the General Assembly, where they are discussed further and adopted. All 193 member countries of the United Nations are represented in the GA 1st.
The history of the General Assembly and its main committees goes back to the founding days of the United Nations. While the name and priorities of the First Committee have seen changes over the years, it has always dealt with security-related issues. Disarmament, conflict prevention and stability are as relevant today as they were 73 years ago, when the UN was founded.
The GA 1st is a relatively new committee at OLMUN. It was first simulated in 2017, when it dealt with "Tackling the Threat of Biological and Chemical Weapons". At OLMUN 2018, the topic will be "Developing Counter-Measures Against Cyber Warfare".

3. Developing Counter-Measures Against Cyber Warfare

This part of the guide gives you a general overview of the topic and past action by the international community.

3.1 Introduction to the issue

From the earliest days of mankind onwards, warfare has been used to settle disputes between groups and to exercise power over others. Just as technology evolved with human development over the centuries, so did techniques of warfare. New computer technology in the 20th and 21st century opened up new ways to attack individuals, institutions or entire countries, as it exposes those that employ it to new kinds of threats.
The term 'cyber' is used as a descriptor for issues related to computer systems and networks. 'Warfare' refers to acts and activities of war. 'Cyber warfare' describes the use and targeting of digital networks, computers, and online systems for the purpose of warfare, through so-called 'cyber-attacks'. Cyber-attacks are usually used to disable websites, networks or computers, steal, alter or destroy confidential data, and disrupt or disable digital systems. To turn a cyber-attack into an act of war, it has to target a country's critical infrastructure. As cyber-attacks generally happen remotely and abuse flaws and weaknesses in digital systems, an experienced attacker requires not more than a computer and an internet connection. Only large-scale attacks that rely on sending large amounts of data quickly require data centres. This makes it incredibly difficult to identify potential sources of cyber-attacks. In recent years, the number of cyber-attacks has seen a significant increase but is usually carried out by ordinary criminals for financial gain. As more and more countries are growing their cyber attack and defence capabilities, and terrorist organisations adopt such attacks as a weapon of choice, the risk of having cyber-attacks used for warfare increases.

3.2 History of cyber warfare

The first computer viruses, which in-itself are a form of cyber-attack, appeared in the 1970s. With the evolution of digital technology and computer security systems, cyber-attacks have also become more sophisticated.
The widespread use of cyber-attacks for political purposes became common from the early 2000s onwards. In 2008, hackers managed to get access secured computers of the United States' Pentagon. The USA blamed the Russian government for the attack. The same year, a virus was also found in the computers of the International Space Station. Nowadays, countries experience attacks against government, military and intelligence service computers on a daily basis. Western countries generally assume China or Russia as the source of those attacks, although North Korea has been named as a possible perpetrator as well.
The first publicly known "cyberweapon" was Stuxnet, a malware computer programme believed to be developed by the United States and Israel. In 2010, Stuxnet was used against nuclear centrifuges in Iran that were being used for

the enrichment of uranium. Stuxnet caused the centrifuges to spin faster than intended, destroying themselves in the process.
In 2013, it was revealed through a leak of top secret documents that the National Security Agency (NSA) of the United States of America had created a global network of surveillance. The NSA's surveillance, aside from collecting personal information about the general population, also included wiretapping the phones of government officials, hacking government computers, installing secret listening devices in embassies, and industrial espionage.
While the origin of cyber-attacks is often unclear, it is commonly believed that China, Israel, the United States and Russia have the most advanced cyber warfare capabilities.

3.3 Types and purposes of cyber-attacks

Cyber-attacks can be distinguished by the aim of the attack: Disclosure of data, manipulation of data, taking control of the system, or disabling the functionality.
In case of disclosure of data, the attacker aims to get access to information that is saved on a computer system, but only accessible to authorised users. The attacker attempts to bypass the authentication process of the system, usually a password. If successful, this can be used in cyber warfare to gain access to classified documents.
Manipulation of data works in a similar way, but instead of simply stealing information, the goal is here to change it on the targets system. To avoid restoration of the data to its original state, attackers usually want to keep their forgery undetected. In warfare, this can be used to make the target act on wrong information.
Taking complete control of a computer system is the most difficult to execute kind of cyber-attack. The attacker attempts to hijack the system, gaining full access to and control over all functionality. This can enable the attacker to execute tasks that even an authorised user would not be allowed to do. In warfare, hijacking of computer systems can be used to cause significant damage to vital public or military infrastructure by using it against its owners.
The last kind of attack is generally seen as the simplest, and there are many different approaches to achieve it. Disabling the functionality of a system, commonly referred to as 'Denial of Service', aims to temporarily or permanently stop a computer system from doing what it is designed to. The ways an attacker can achieve this range from overloading a system with an abundance of information, to finding ways to surgically disable a system. In warfare, this can be used to disable or destroy your targets defences and infrastructure.
Possible targets of cyber-attacks that can interpreted as acts of war include, but are not limited to:
- Turning off the water and energy supply of a country
- Stealing state secrets
- Manipulating military intelligence
- Hacking voting machines to change the result of an election
- Getting access to surveillance cameras
- Disabling weapon systems
- Taking over computer-controlled weapons

The damage caused by cyber-attacks is often economic or weakens existing defence systems. For that reason, it is unlikely that cyber warfare will ever replace conventional weapons. However, cyber-attacks can often not be directly attributed to an actor and are therefore easy to deny. This characteristic makes them suitable to test an opponent's defences in a cold war scenario, or for the usage by terrorist organisations. Even systems that are not connected to the internet can become victims of cyber-attacks. This requires a physical introduction of a virus, for example through a USB drive.

3.4 Cyber terrorism

Ever since cyber-attacks became a common threat, some countries have expressed the fear that terrorist organisations, such as ISIL (Islamic State of Iraq and LEevant) or Al Qaeda, could use cyber-attacks for their purposes. A scenario for possible 'cyber terrorism' could be an attack on a nuclear power station that causes an explosion of the reactor. However, no major attempted or successful cyber terrorism attacks are known, and it is questioned by some whether those terrorist groups can be able to gain the expertise required.

3.4 International response

With the rise of harmful cyber-attacks, the United Nations has started including the prevention of them in their disarmament efforts. Pursuant to the General Assembly resolution 66/24, an international Group of Governmental Experts worked on recommendations. They agreed in 2013 that international law should also apply to cyberspace, which would make cyber-attacks against other countries the same as conventional acts of war. In 2015, the group also agreed that countries should be held responsible for actions that originate from their territory and should assist each other in investigation cyber-attacks. However, there have so far been no UN resolutions or conventions that ban, limit or at least provide a legal framework for cyber warfare.

Since there is no uniform international approach, many member states have taken measures on a national level or through regional and intergovernmental organisations to protect themselves against cyber-attacks. Those measures usually consist of specialised personnel, which monitors potential threats, mitigates them, and attempts to track them to their origin. As the security of IT systems improves, attackers are constantly looking for new vulnerabilities to exploit. While smaller and less-developed countries usually have a lower number of computer systems and networks that can be potential targets of cyber-attacks, they often also lack the resources to develop their own counter-measures. According to the Global Cybersecurity Index by the International Telecommunication Union, only 38% of UN member countries had developed a cybersecurity strategy.

In the Charter of the United Nations, promoting peace and security is enshrined as one of its fundamental purposes. With the growing usage of cyber-attacks by state actors, and the resulting tensions and conflicts between them, many experts believe that the time has come for actions.

3.5 Guiding questions

The following questions are meant to guide your research and help you prepare for the topic. All questions are focussed on your country's situation and the solutions supported by your government.

- Does your country have digital infrastructure that could be vulnerable to cyber-attacks?
- Has your country been accused of carrying out cyber-attacks?
- Is your country in favour of strict rules for disarmament?
- Has your country been victim of a major cyber-attack?
- What national measures has your country taken to protect itself against cyber warfare?

3.6 Useful links for further research

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Global Cybersecurity Index (GCI) 2017
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

UN Secretary-General calls for rules for cyber warfare (article)
https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4