MEET THE BOARD OF DISEC COMMITTEE - PUCPMUN 2019

DIRECTOR:

Dear delegates,
Welcome to PUCPMUN!

My name is Milene Chagua Zúñiga and it’s a pleasure to being your Director at the Disarmament and International Security Committee (DISEC) in the ninth edition of PUCPMUN.

I'm a senior year Law student at National University of San Marcos who has recently been admitted at University of Montreal in Canada. I started my MUN experience in 2016, when I was a member of Delegación Internacional San Marcos (DISM) I've participated as a delegate in PUCPMUN 2016 and USILMUN 2016; as a faculty advisor in PUCPMUN 2017; and this will be my first time in chair.

Participating in MUN, increased my interest in diplomacy and international organizations as well as Public International Law, Humanitarian International Law and Intellectual Property, which are the main subjects of my speciality. The biggest challenge in my career was participate in the 60th edition of Philip C. Jessup International Law Moot Court Competition 2019 "The Case concerning The Kayleff Yak " in Washington DC, which is a simulation of a fictional dispute between two States before the International Court of Justice. I had the honor of representing my country as oralist of the Applicant and competing with around 130 teams of every part of the world that experience made me realize how much I love International Law.

This year DISEC Committee will address “Cyber Warfare”, a new issue that got immediately the attention of the international community and call for adequate measures in order to maintain world security. As a recent topic, I’m so excited to look forward to a great level of debate in my committee and that debate leading you to unfold all your creativity to reach the most innovative proposals and effective solutions.

I will do my best to make this committee as interesting and dynamic as possible. Make sure to bring the best you have! See you soon!

Kind regards,

Milene Chagua

milenecz.17@gmail.com
ASSISTANT DIRECTOR:

My name is Gabriela Rodríguez Coronado, but most people simply know me as Gaby and I have the pleasure of being your director for this edition of PUCP MUN. I have a bachelor's degree in Commercial Engineering with a specialty in International Business from the Catholic University of Santa María. This career captures my passion for management and decision making as well as my vocation for service. I love music, I've dedicated my whole life to it. I think I'm a quaver in the perfect musical score, which I call life. I love pizza, hot chocolate, and politics; I'm from Lima. However, I grew and lived almost my entire life in Arequipa, land that I love as if it were mine. In 2014, I participated in my first MUN and learned the importance of diplomacy and ethical competence. I felt each of the topics as something transcendental that should continue to grow in favor of safeguarding the rights and well-being of people. Then, I traveled to the United States and in the college where I studied, they taught me something that remained engraved in me since then as an axis in my life. The phrase “think global, act local”, Today, in my life, it is a reality, and I know for sure that it is in yours, because being a munner in our city is something not very known or attractive, but it is a first step to make a big change. I firmly believe that you must be the change you want to see in the world.

Outside of the MUN, I am a fan of Disney movies and also of the entire Harry Potter world. Netflix's number one fan, although it does not have all my favorite movies. I like to cook, especially desserts; and for 5 years, I spend my afternoons with my loyal friend, whose name is Nemo. I love music, I play different instruments and I love singing, I think there is no better way to spend the days if you do not sing your favorite song.

I am very excited to be part of your board of directors on the DISEC committee, where we will explore the issue of cyber warfare, a matter of vital importance as it requires new measures to preserve global security. I hope that this committee can be an enriching experience for all, that the debate be competitive and conscious in decision making, taking into account the importance of the proposals and solutions.

I'm waiting for you in this incredible edition of PUCP MUN 2019!!!!!!

Gabriela Coronado
gaby.25796@gmail.com
Hi delegates!
My name is Marcela Campos and I am really excited for this upcoming conference. I am a senior year Law student at the Universidad de San Martin de Porres. I discovered MUN thanks to my best friend in 2017, since then I have been participating in national and international conferences (HNMUN-LA, Harvard WorldMUN and HNMUN). My last experience was HNMUN 2019, and I really enjoyed it. This will be my second time moderating a high school committee, the first time the delegates surprised me and I am sure you will do it too.

Cyber warfare is such a technical topic to discuss, and I want you to be the experts. I hope this guide will serve you to discover your path through this amazing topic and we will allow you to be as creative as you can. Remember that to solve issues of this magnitude, we need you to be one step ahead.

Have fun, play fair and connect with people.

Looking forward to meet you all!

Kind regards,
Marcela Campos
marcelacammer@gmail.com
INTRODUCTION TO THE COMMITTEE

After damage and atrocities left as a result of the two World Wars, the United Nations member States took the disarmament and security as core aspects since its foundation, and the emphasis on these main aspects has led to the creation of The Disarmament and International Security Committee (DISEC), the first committee of the UN General Assembly that deals with disarmament, global challenges and threats to peace that affect the international community and seeks out to the solutions to the challenges in the international security regime.

It considers all disarmament and international security matters relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The First Committee provides space for each state to discuss its positions related to disarmament. It offers states the opportunity to build consensus on issues, therefore, instead of guaranteeing security through the size of their arsenals, governments can discuss the best way to reach cooperative security agreements that minimize spending in arms, reduce arms production, trade and reserves, and increase world security. This consensus can be used later in other disarmament forums, such as the Conference on Disarmament, where disarmament treaties are negotiated.

However, there are doubts about what DISEC Committee can do that Security Council (SC) could not. The main difference comes in the process in which both operate, owing to the fact that it is a General Assembly with a range of countries and they are not limited to 15 members; though the SC is the only UN body able to imposing force upon Member States, DISEC Committee makes valuable recommendations to the SC on all aspects concerning global peace. Due to, there are not a veto power resolutions must be passed with majority. DISEC is ordered to focus on security and disarmament issues and work in cooperation with the United Nations Disarmament Commission and the Conference on Disarmament, which are highly specialized organs that provide them with up to data information.

Through discussion and cooperation, DISEC delegates will take appropriate measures for increasing the capacity to manage the issue of cyber warfare.
DEFINITION OF CYBER WARFARE

Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target. ¹

The most distinctive characteristics of cyber warfare are:

- Cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict.
- Cyberspace gives disproportionate power to small and otherwise relatively insignificant actors.
- Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.
- In cyberspace the boundaries are blurred between the military and the civilian, and between the physical and the virtual; and power can be exerted by states or non-state actors, or by proxy.
- Cyberspace should be viewed as the ‘fifth battlespace’, alongside the more traditional arenas of land, air, sea and space. Cyber warfare is best understood as a new but not entirely separate component of this multifaceted conflict environment.
- Warlike actions in cyberspace are more likely to occur in conjunction with other forms of coercion and confrontation. However, the ways and means of cyber warfare remain undeniably distinct from these other modes of conflict.

An Early Warning System (EWS) is technology and associated policies and procedures designed to predict and mitigate the harm of natural and human-initiated disasters and other undesirable events. Early warning systems for natural hazards include those designed for floods, earthquakes, avalanches, tsunamis, tornadoes, landslides, and drought. Other systems exist for a variety of events including missile launches, road conditions, and disease outbreaks. The United Nations International Strategy for Disaster Reduction (ISDR) recommends that early warning systems have the following four components:

- **Risk knowledge**: Data should be systematically collected and analyzed and risk assessments performed.
- **Monitoring and warning service**: Systems should be in place to monitor hazards and provide early warning services.
- **Dissemination and communication**: Risk information and early warning messages must be delivered.
- **Response capability**: Systems should be in place to respond to events, build national and community response capabilities.

In IT (information technology), early warning systems are used in a variety of environments.

Each U.S. military service has its own written definition for what comprises a weapon. However, a “weapon” must also meet international legal standards. The Hague and Geneva conventions describe how a “capability” that is called a weapon cannot legitimately be used by the military until after a legal review. These conventions are intended to protect the civilian population from unnecessary suffering during a war.

According to the "Tallinn Manual on International Law Applicable to Cyber Warfare" developed after a series of cyber attacks directed against Estonia in 2007, it defines a cybernetic weapon as a "cybernetic means of war" that are by design, use, or intended use capable of causing either injury to, or death of persons; or damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack. The term means of cyber warfare encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, material, instrument, mechanism, equipment, or software used, designed or intended to be used to conduct a cyber attack.

So, if there is an intentional injury, or if the functionality of the computer is intentionally interrupted through a cyber attack, then we may be experiencing a cybernetic weapon.

---

ONGOING ISSUES RELATED TO CYBER WARFARE

Terrorism and extremism
In response to the growing trend in violent extremism and the minimal focus that was being afforded to preventive efforts in the Counter-Terrorism Strategy, in January 2016 the United Nations Secretary-General presented a Plan of Action to Prevent Violent Extremism to the General Assembly.\(^5\) In the Plan, the Secretary-General calls for a comprehensive approach encompassing not only essential security-based counter-terrorism measures but also systematic preventive steps to address the underlying conditions that drive individuals to radicalize and join violent extremist groups. The Plan is an appeal for concerted action by the international community, providing some 70 recommendations to Member States and the United Nations system to prevent the further spread of violent extremism, and includes an entire section on “Strategic communications, the Internet and social media”.\(^6\) A first conference was organized in Geneva in April 2016 for the international community to share experiences and good practices on how to prevent violent extremism. However, while there was a certain emphasis on the need to engage with the online 43 dimension of violent

---


extremism and link it to off-line efforts, there was limited participation of relevant technology and social media companies in the conference deliberations.\(^7\)

**Psychological cyber warfare**

There can be a psychological dimension to cyber attacks. The infiltration of what are assumed to be secure systems and critical infrastructure highlights national vulnerabilities and weaknesses. This can provoke feelings of insecurity, as evidenced by the Stuxnet worm in Iran and the Titan Rain episodes in the United States and the United Kingdom. Engendering this sense of insecurity could indeed be the attacker’s goal, in the same way that the fear of terrorism and its potential harm can have a detrimental and disabling effect almost as great as the terrorist act itself. Indeed, according to Dennis Murphy, ‘some observers equated that cyber attack [on Estonia in spring 2007] to an act of war in the Clausewitzian sense, with the intent to create mass social panic’\(^8\).

**Economic cyber crime**

The Center for Strategic and International Studies (CSIS), in partnership with McAfee, presented “Economic Impact of Cybercrime – No Slowing Down”, a global report that focuses on the significant impact that cybercrime has on economies worldwide. The report concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year, which is up from a 2014 study that put global losses at about $445 billion. The report attributes the growth over three years to cybercriminals quickly adopting new technologies and the ease of cybercrime growing as actors leverage black markets and digital currencies\(^9\).

**Cyber espionage**

Cyber spying is the act of engaging in an attack or series of attacks that let an unauthorized user or users view classified material. These attacks are often subtle, amounting to nothing more than an unnoticed bit of code or process running in the background of a mainframe or personas workstation, and the target is usually a corporate or government entity. The goal of this action is typically to uncover sensitive government information, steal trade secrets or commercial data or acquire intellectual property. This kind of attacks can be motivated by greed or profit, and can be used in conjunction with a military operation or as an act of terrorism. As a consequence, there could be from loss of competitive advantage to loss of materials, data, infrastructure, or loss of life\(^10\).

---


\(^8\) Murphy, “*Attack or defend?*”, p. 91 obtained from: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf


\(^10\) Villanova University. What is Cyber espionage? obtained from https://www.villanovau.com/resources/iss/cyber-espionage/
MEASURES ALREADY TAKEN

International law regarding real warfare developed within a 150 years. This raises the question whether these regulations could be used in matters of online-warfare. A genuine legal framework, a *jus ad bellum* and *jus in bello*, is still missing for cyber warfare. The Working Group on Internet Governance, established by the United Nations based on a recommendation from the World Summit on the Information Society, was initiated to agree upon the future Internet Governance. Technical, policy, economic, institutional, as well as legal perspectives were taken into consideration. Two different approaches dominated the debates at the summit. Whereas one side argued for the development of genuine cyber-law since speed and volume of Internet cross-border communication hinders the enforcement of existing legal rules, the other side argued that the Internet is in fact not conceptually different from previous telecommunication technologies. Consequently, existing legal rules could be applied to the Internet and as far as global regulation is concerned, the most efficient option would be the harmonization of national laws, resulting in the establishment of one set of equivalent rules at the global level.

The Working Group has fulfilled its duty to give recommendations for the next World Summit on the Information Society. But unfortunately a consensus regarding concrete measures could not be found. For the time being, bilateral agreements are the most common solution for cyber security regulations, like the new security pact of the UK with India. A group of international lawyers, working in conjunction with the International Committee of the Red Cross and the US Cyber Command, has now published a book on the subject. The group of experts was invited to draw up the handbook by NATO’s Co-operative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, where the centre was established in 2008 following a wave of cyber-attacks on the Baltic state from inside Russia. The experts explained that existing laws broadly apply to cyberspace. The Tallinn manual contains 95 “black letter rules”.

However, there is no official NATO document or policy but an advisory manual. Among other things it stipulates that cyber attacks led by governments must avoid sensitive civilian targets such as hospitals, dams, dykes and nuclear power stations. The manual also states that “hacktivists” who participate in online attacks during a war can be legitimate targets even though they are civilians. The manual suggests “proportionate countermeasures” against cyber attacks carried out by a state are permitted. Such measures cannot involve the use of force, however, unless the original cyber-attack resulted in death or significant damage to property.” Rule seven of the manual also states that if an online operation originates from a government network, "it is not sufficient evidence for attributing the operation to that state but is an indication that the state in question is associated with the operation". Furthermore, it says that, in accordance with the Geneva Conventions, attacks on certain key civilian sites are
outlawed, for instance hospitals and medical units, which are also protected under rules governing traditional warfare.

**BLOC POSITIONS**

We strongly suggest you to look upon regional bodies, international and bilateral agreements in order to act according to your country's policy. This section only provides you a hint about some actors and alliances that are well known when talking about cyber security.

It is impossible to provide a complete map of intelligence sharing arrangements in place around the world. One of the best known sharing arrangements is the Five Eyes alliance between the US, UK, Australia, Canada and New Zealand. But despite being over 70 years old, little is known about the alliance, including the current agreement(s) that govern it\(^\text{11}\).

The Nine Eyes countries include: 5 Eyes countries, Denmark, France, the Netherlands and Norway. The existence of the Nine Eyes alliance is referenced in various sources online and became well-known following the Snowden revelations in 2013. It is just an extension of the Five Eyes alliance with similar cooperation to collect and share mass surveillance data.

The 14 Eyes surveillance countries include: 9 Eyes countries, Germany, Belgium, Italy, Sweden and Spain. As before, the original surveillance agreement was extended to these

other countries. The official name of this group of countries is referred to as SIGINT Seniors Europe (SSEUR)\textsuperscript{12}.

There is evidence suggesting that Israel, Singapore, South Korea, and Japan are additional partners of the above mentioned alliances, but this is unconfirmed, isn’t it?

NATO is developing a military command center to deter computer hackers, while experts say Russia, North Korea and China are also constantly deploying sophisticated computer hacking weapons and surveillance software\textsuperscript{13}.

According to the Internet Security Threat Report 2018 (ISTR) by Symantec, Brazil and Mexico rank 7th and 8th regarding most ransomware attacks worldwide, while Brazil, Argentina, and Mexico occupy globally the 3rd, 8th and 10th place in country of origin in cyberattacks\textsuperscript{14}.

![Image of a globe with interconnected circuits]

Cybercriminals often use unprotected computers to launch cyberattacks against targets all over the world. This is the main reason why countries with less developed policies on cyber security are not off the hook.

We need to ensure prevention systems, protocols during an attack and contingency plans.

\textbf{QARMAS}

\textsuperscript{12} https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/
\textsuperscript{14} https://www.symantec.com/security-center/threat-report
1. How could the committee ensure security of cyberspace?
2. What role do foreign powers such as the P5 and European Union have in the solution of the topic?
3. How do we ensure that cyber terrorism cannot produce risks to environment, national or international economy and people’s life?
4. How to manage digital risks?
5. What the response should be in the event of an ICT incident?
6. How to enhance the solutions proposed with the other UN bodies?

SUGGESTIONS FOR FURTHER READING

Online files:


FINALS ADVICE

- Be sure of your speaking skills and be confident about what you are saying.
- Do not limit your research to this study guide only. The present study guide plays an essential part in terms of groundwork for the committee but you must be well prepared and carry out in depth research of the topic.
- You should know the basics about your country, foreign relations with other countries and you allies, also you must conduct a research in the stance and the impact these issues have had on your country and their involvement over time.
- Research the most recent developments on the issue and any action that have been taken.
- Find and use facts and figures about your country’s stance to support your points.
- Make sure you support your country’s stance on the topic based on its Constitution, never go off- policy or against your country’s stance.
- Maintaining the decorum is the most essential part. Do not interrupt a person when they have been recognized to speak.

We invite you to take risks, learn and nurture your knowledge on the subject. MUN simulations are an academic learning tool which allows us to grow as future professionals and
consider realities that are different from our own lives. You are welcome to contact us with any questions you have or about any information you need.

We look forward to seeing your skills of diplomacy and leadership. We hope to give you a memorable experience at PUCPMUN 2019 that you can be proud of.