PIMUN
2022 !

STUDY GUIDE DISEC

"Curbing the global threat of Cyberterrorism"

LETTER FROM THE CHAIRS

Dear Delegates,

Welcome to Paris International Model United Nations 2022 and the Disarmament and Security Council !

We are more than happy to be able to simulate one of the most important committees existing today in order to be able to discuss one of the most important global issues occurring globally.

As your chairs, we promise to do our best to bring you a fruitful and efficient committee simulation despite the unforeseen circumstances happening as a result of the current pandemic.

We believe that you are resilient delegates that will be able to make the most out of their own experience and, most importantly, have fun while doing just that!

Please keep in mind that we are discussing a very crucial issue in our world today and it requires your utmost care and dedication. Remember that you are the leaders of tomorrow!

Research as much as you can in order to be able to write the best possible resolution you can throughout the conference.

We believe in you, and we cannot wait to meet you soon.

All the best,

The DISEC, Board of Directors

INTRODUCTION TO THE CHAIRS

Introduction to the Chair (Dylan Breyne)

Hello everyone ! My name is Dylan and I am really honoured to be your chair for DISEC. I am a first year master's student at the University Jean Moulin Lyon III studying International Relations, specialising in international security. I am an academic at heart - I love art, reading, nature, all the sciences, and have a particular interest in diplomacy and outer space affairs.

I am originally from Paris, and I moved to Switzerland when I was a kid. I’ve travelled all around the world and started my MUN journey back in London at my high school. At first, I was confused yet excited as well, and as the years went by I quickly fell in love with the simulations and couldn’t stop myself. Next thing I knew, I was joining my university MUN club and being able to even debate at the headquarters of the UN in Geneva.

I can’t wait to meet you all and make sure that DISEC is the best committee at PIMUN 2022!

INTRODUCTION TO THE COMMITTEE (1) :

The Disarmament and Security Council (DISEC) is the First Committee of the United Nations General Assembly, established as such with the creation of the United Nations in 1945. DISEC contains two main bodies that report to it: the Disarmament Commission (UNDC) and the Conference on Disarmament (CD). Although the CD is not technically a part of the UN, it still reports to DISEC and its budget is included in that of the UN.

DISEC mainly deals with the broad issues of nuclear weapons and other weapons of mass destruction, outer space, conventional weapons, regional disarmament and security, other disarmament measures and international security, and disarmament and security. DISEC has had a few landmark resolutions, including the very first General Assembly resolution "Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy" in 1946.

In addition, DISEC has passed the very first General Assembly resolution that was co-sponsored by all the Member States of the time. This resolution, adopted in 2001, reaffirmed all resolutions on the situation in Afghanistan and confirmed that the United Nations would play an important role in the country. It also called for the establishment of a transitional administration leading to the formation of a new government.

Keep in mind that all resolutions passed by this committee are non-binding resolutions and must be formatted as recommendations to the 193 nations in the committee.

Furthermore, given its direct association with the United Nations General Assembly (being a subsidiary organ as authorised under Article 22), it retains the powers and responsibilities of the General Assembly as outlined in Chapter IV of the Charter of the United Nations, including:

- **Article 10**
  "*mak[ing] recommendations to the Members of the United Nations or to the Security Council or to both on any such questions or matters.*"
- **Article 11(2)**
  "*discuss[ing] any questions relating to the maintenance of international peace and security brought before it...*"

[1] *UN General Assembly - First Committee - Disarmament and International Security*. (n.d.). the United Nations. Retrieved March 18, 2022, from https://www.un.org/en/ga/first/index.shtml

- **Article 11(3)**
  "*call[ing] the attention of the Security Council to situations which are likely to endanger international peace and security.*"
- **Article 14**
  "*recommend[ing] measures for the peaceful adjustment of any situation...*"

As delegates at PIMUN 2022, you should keep in mind these values of international cooperation and the promotion of world peace as you work to craft solutions to this issue, which is extremely important to the promotion of international security.

1. Introduction to the Topic:

Cyberterrorism has captured the attention of the media, the security community, and the information technology (IT) industry. Journalists, legislators, and professionals in a variety of fields have popularised the idea of sophisticated cyberterrorists electronically breaking into computers that regulate dams or air traffic control systems, creating havoc and jeopardising not only millions of lives but also national security. Despite all of the dire forecasts of a cyber-generated catastrophe, no single case of actual cyberterrorism has been documented.

How serious is the threat posed by cyberterrorism? Because the majority of essential infrastructure in Western society is networked via computers, the potential threat from cyberterrorism is, to say the least, concerning. Although hackers are not driven by the same goals as terrorists, they have proved that anybody can get access to sensitive information and the operation of critical systems. Terrorists may, in theory, follow the hackers' lead and, after breaking into government and commercial computer networks, cripple or at least paralyse industrialised countries' military, financial, and service sectors. Our society' increasing reliance on information technology has produced a new type of vulnerability, allowing terrorists to attack targets that would otherwise be completely impenetrable, such as national defence systems and air traffic control systems. The more technologically advanced a country is, the more vulnerable its infrastructure is to cyberattacks.

Concerns regarding the possible threat posed by cyberterrorism are thus warranted. That does not mean that all of the concerns expressed in the media, Congress, and other public forums are fair and acceptable. Some anxieties are simply unfounded, but others are greatly overblown. Furthermore, the gap between potential and actual damage perpetrated by cyberterrorists has too often been overlooked, and most hackers' comparatively benign actions have been confounded with the threat of pure cyberterrorism.

This guide can provide a brief overview of the current and future reality of the cyberterrorism threat including some past relevant action on the same. It begins by explaining why cyberterrorism anxiety has gripped so many people, defines what constitutes "cyberterrorism" and what does not, then charts the appeal of cyberterrorism to terrorists.

2. Key Definitions:

Cyber security : There are two definitions of cyber security. The first is concerned with the security of information systems against theft or damage to the hardware, software, and data stored on them, as well as disruption or misdirection of the services they provide. The second refers to the product that results from the collection, processing, integration, evaluation, analysis, and interpretation of available information about foreign states, hostile or potentially hostile forces or elements, or areas of actual or potential operations; the activities that result in the product; and the organisations that engage in such activities.

Cyberterrorism : Cybersecurity and New Technologies programme aims to enhance capacities of Member States and private organizations in preventing cyber-attacks carried out by terrorist actors against critical infrastructure.

Cyber Crime : Cybercrime is defined as a crime in which a computer is either the object of the crime or is used to commit the crime. A cybercriminal may use a device to gain access to a user's personal information, confidential business information, government information, or to disable the device. Selling or obtaining the aforementioned information online is also a cybercrime.

Cyber Threat : A cyber threat is a malicious and destructive act that attempts to gain access to a computer network via a data communications pathway without the proper authorization or consent from the owners. With the introduction of personal computers, cyber threats entered the spotlight.

Hacktivism : A mix of “hacking” and “activism”, could be delineated as the activity of getting into computer systems and wreaking havoc in order to achieve political aims or social changes.

Malware : Any kind of computer program intended to cause damage or disruption to a system.

Non-State Actor: An organization that is not a country, typically used in the context to delineate between states and non-states, non-states normally being far more limited in their capabilities.

State Actor: A country (as opposed to an organization), that has typically more capabilities than any organization.

3. Problems Identification:

Absence of a clear definition

First things first, there is no clear definition of terrorism in international law. And despite many attempts on the United Nations, States have not yet agreed upon a definition of terrorism. The reason behind is simply because one man’s terrorist is an other man’s freedom fighter : the term terrorism has political and ideological connotations. Subsequently, there is no definition of what cyberterrorism is.

There have been several roadblocks to developing a clear and consistent definition of "cyberterrorism." First, as previously stated, much of the discussion of cyberterrorism has taken place in the popular media, where journalists are more concerned with drama and sensation than with good operational definitions of new terms. Second, when dealing with computers, it has been especially common to coin new words simply by associating the words “cyber", "computer," or "information" to another word. Thus, a slew of terms-cybercrime, infowar, netwar, cyberterrorism, cyberharassment, virtual warfare, digital terrorism, cybertactics, computer warfare, cyberattack, and cyber-break-ins—are employed to describe what some military and political strategists refer to as the "new terrorism" of our times.

Fortunately, some attempts have been made to improve semantic precision. Most notably, Dorothy Denning, a computer science professor, has proposed an admirably unambiguous definition in numerous articles and in her testimony before the House Armed Services Committee in May 2000:

The fusion of cyberspace and terrorism is known as cyberterrorism. It refers to unlawful attacks and threats of attacks on computers, networks, and the information stored on them that are carried out in order to intimidate or coerce a government or its people in the pursuit of political or social objectives. Furthermore, in order to qualify as cyberterrorism, an attack must result in violence against people or property, or at the very least cause enough harm to cause fear. Attacks resulting in death or bodily harm, explosions, or severe economic loss are examples. Depending on the severity of the attack, serious cyberattacks against critical infrastructures could be considered acts of cyberterrorism. Attacks that disrupt non-essential services or are primarily a costly nuisance would not be tolerated.

Difficulty to identify the authors

Another vital point to keep in mind regarding cyber attacks is that it takes time to find and to identify the author behind a cyber attack, and most of the time there is no possibility to be one hundred percent sure of who or what is responsible for the cyber attack. And even with tangible proofs, a State will, most of the time, simply deny accusations such as the cyber attack on Estonia in 2007. In the case of non-state actors, such as Anonymous for exemple, will be considered as "hacktivists" for some actors and public opinions, whilst they could be considered as terrorists for others stakholders. Hence, the main issue with cyber terrorism and potential cyber terrorists is that, in conflict studies, a terrorist aims to claim high that he is the author, whereas a cyber attack aims to remain hidden and noiseless such as the Stuxnet case showed. So, considering how terrorism functions and how cybersecurity works, some will simply state that cyber terrorism doesn't exist, or doesn't exist yet, claiming that a state actor will always be behind major cyber attacks, terrorists themselves lacking means to lead such actions.

The malicious use of the internet

The malicious use of internet in general via ICTs, which could lead to cyber attacks by terrorists, also raises an issue on its own. The UN Secretary-General Antonio Guterres has therefore made the promotion of a peaceful ICT-environment one of his key priorities. In May 2018, the Secretary-General launched his Agenda for Disarmament. In the Agenda, he notes that "*global interconnectivity means that the frequency and impact of cyberattacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time*." He further states that "in this context, malicious acts in cyberspace are contributing to diminishing trust among States." To address these challenges, the Secretary General has included two action points on cyber in the implementation plan of the Agenda for Disarmament : First, the Secretary-General will make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace. And secondly, the UNSG will engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace.

Current Situation

The majority of these cyber-attacks have been attributed to a variety of hackers and a small number of terrorist organisations, but there have been notable attacks by states against other states over the last fourteen years. The following are some prominent examples of attacks in various states designed to disrupt information networks, gain access to critical materials, destroy data, or mislead the public.

- In 2009-2010, the United States and Israel used a virus known as Stuxnet, Flame, or Olympic Games to attack Iranian nuclear enrichment centrifuges at the Natanz nuclear fuel facility south of Tehran. The Stuxnet attack halted 10% of Iran's uranium enrichment capabilities for a full year, delaying Iran's nuclear plans even further.
- Russian meddling in the US presidential election in 2016 can also be viewed as part of a coordinated series of cyber-attacks. This was a large-scale attack involving thousands of Russian bots on social media platforms such as Facebook and Twitter, with the goal of spreading misinformation and garnering support for then-candidate Donald Trump. This included attempting to reach out to teenagers by disseminating political memes and patriotic posts.
- More examples of cyber-attacks on infrastructure have occurred in Ukraine. Russia hacked into Ukraine's Central Election Commission and disabled part of its network three days before the 2014 presidential election.

These and other cyber-attacks show that cyber-attacks can be used to project state power to negatively impact another state, community, or group of people on the other side of the world. Because the victim is unable to quickly identify their attacker, these attacks are much more difficult to defend against.

Cyberterrorism for Terrorists:

Cyberterrorism is an attractive option for modern terrorists for several reasons :

- For starters, it is less expensive than traditional terrorist methods. All the terrorist requires is a computer and an internet connection. Terrorists do not need to purchase weapons like guns and explosives; instead, they can create and distribute computer viruses via a phone line, cable, or wireless connection.
- Second, unlike traditional terrorist methods, cyberterrorism is more anonymous. Terrorists, like many Internet users, use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it difficult for security agencies and police forces to determine the terrorists' true identity. And there are no physical barriers to overcome in cyberspace, such as checkpoints, borders, or customs agents to outwit.
- Third, there is a huge variety and number of targets. The cyberterrorist may target the computers and computer networks of governments, individuals, public utilities, private airlines, and other organisations. Terrorists will find weaknesses and vulnerabilities to exploit due to the sheer number and complexity of potential targets. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to cyberterrorist attacks because the infrastructures and computer systems that run them are highly complex, making it nearly impossible to eliminate all vulnerabilities.
- Fourth, cyberterrorism can be carried out remotely, which is particularly appealing to terrorists. Cyberterrorism necessitates less physical training, psychological investment, mortality risk, and travel than traditional forms of terrorism, making it easier for terrorist organisations to recruit and retain followers.
- Fifth, as demonstrated by the I LOVE YOU virus, cyberterrorism has the potential to directly affect a greater number of people than traditional terrorist methods, resulting in increased media coverage, which is ultimately what terrorists desire.

4. Past Actions:

Cyber security is a relatively new field and has been dealt with in many different manners depending on the country. Overall, there has been a lack of a cohesive approach to combating cyber attacks and repercussions for these attacks. Due to this lack of a cohesive response, the United Nations has also been slow to respond to the rapidly evolving issue of cyber security. The organisation within the UN that is dedicated to addressing the issue of cyber security is the International Telecommunication Union (ITU).

Broadly, the ITU is aimed at protecting, spreading, and advancing information and communication technologies (ICTs). Despite the broad scope of the work, they have done limited work on the issues of cyber security. The ITU only gives reference to five UN resolutions that are related to cyber security : and none of them are especially complex.
Two of the resolutions are about combating criminal misuse of information technology, while the three other resolutions are about building a global culture of cyber security. While the ITU and its member states recognize that cyber security is an important issue that needs to be addressed, it offers limited ways on how to go about doing that.

Yet, despite the lack of action taken by the UN and the ITU, they have proposed some significant solutions and methods to secure cyberspace. In 2007, the ITU created the Global Cyber Security Agenda (GCA) which is built upon five pillars: legal measures, technical and procedural measures, organisational structures, capacity building, and international cooperation. However, even with the work of the GCA, the world is still lacking a coordinated attempt to address cyber security as a whole.

Following the 11 September 2001 New York City terrorist attacks, the Security Council created the Counter-Terrorism Committee (CTC) and its Executive Directorate (CTED) through Security Council resolution 1373 (2001), with the mandate to strengthen Member States' capacity to combat terrorism through capacity-building mechanisms (S/RES/1373 (2001). Alongside with the General Assembly First Committee, with a mandate to promote and maintain international peace and security, those institutions are crucial actors in combating terrorism.

Another UN organisation aimed at addressing cyber security is the United Nations Institute for Disarmament Research (UNIDR). The UNIDR is behind the publication of the Cyber Security Index, an overview of international cyber security that is accompanied by text to help clarify cyber security and explain its importance and the importance of implementing policy surrounding it. This tool is extremely useful because it helps broaden understanding of the issue, a key barrier to effectively addressing cyber security.

Even if UN organizations like the Economic and Social Affairs Committee (ECOSOC) have warned of the potential risks of cyber security but have provided a limited plan on how to go about combating cyber threats, concerning terrorism, the UN possess a large number of tools and institutions aiming to tackle this issue.

5. Possible Solutions :

Over the course of the debate, delegates and their blocs should be working to address and provide solutions to questions such as: How can we put in place regulations to address nations interacting with the cyber infrastructure of other nations or non-state actors? How can we protect nations and their citizens from cyber attacks, ranging from cyber crime to cyber terrorism in an increasingly digital age?

These questions are broad, and an ideal resolution should address the smaller details within each problem that is posed. It is also alright if a resolution does not address all these areas in the same depth, but you can use the questions above as a general guideline for steering your conversations and research.

In the end, to effectively address the emerging challenges of cyber threats to peace and security and their effects on development that could lead to cyber terrorism, possible solutions must involve collaboration between all stakeholders, including the United Nations Secretariat, Agencies, Funds and Member States, as well as external partners, including academia, the public and private sectors and the public.

A possible resolution will lead efforts to build capacity, strengthen coordination and foster collaboration to enhance cybersecurity preparedness, resilience and response. Furthermore, encouraging States and non-state actors to finally agree upon a definition of terrorism and subsequently, cyber terrorism would be very much in order.

"*The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.*" Ban Ki-moon, previous Secretary General of the United Nations.

6. Bloc Positions :

Per se, every countries present in this committee will agree on the fact that terrorism is an issue threatening international security and as such, must be tackled. Moreover, cybersecurity is essential, guaranteeing citizens' rights and peace in technology advanced or developing countries. Processes and methods will however diverge depending on different diplomatic positions :

On one hand, you can identify "pro cyber warfare and conditional civil liberties" which, most likely, countries in this bloc will be western democracies that wish to guarantee the private rights and securities of individual citizens, but only to a certain extent. Additionally, these countries will have either been victims and/or perpetrators of cyber warfare and see this practice as the future of modern warfare. Countries like this may include nations such as the United States of America, the United Kingdom, France, and more.

On the other hand, you will have the "pro cyber warfare and security first" : those countries in this bloc will most likely be authoritarian governments that wish to control the cyber capabilities of its citizens. Additionally, these countries will have either been a victim and/or perpetrator of cyber warfare and see this practice as the future of modern warfare. Countries like this may include nations such as China, Syria, Egypt, Venezuela, and more.

Then, it is also possible to identify two more blocs : "Anti cyber warfare and high civil liberties" or countries that will also most likely be western democracies, as in the first bloc, but will instead put an absolute premium on individual civil liberties, without exceptions. These nations will also wish to restrict cyber warfare as they wish to protect their citizens not only from the heavy hand of their own government but from other governments as well. These nations may include countries such as New Zealand, Switzerland, Denmark, and more.

And last but not least, a final bloc that you could call “technologically developing nations”: Not all nations have a great cyber presence. Developing nations in particular struggle with creating and maintaining technologically advanced infrastructure. Nations in this bloc will most likely wish to support expanding cyber infrastructure to underdeveloped nations and set up cyber security against cyber threats, which may be even more damaging here due to the lack of an adequate cyber infrastructure.

These nations may include nations that are still developing a cyber infrastructure, such as Togo, Botswana, Eritrea, etc.

7. QARMAs:

- How should member states respond to the potential threat posed by non-state actors acquiring offensive cyber technology, potentially leading to cyber terrorism?
- What principles can guide an international agreement on the limitations of information technology use for the sake of international peace and security?
- How could capacities be built to identify, prevent and respond to cyber threats? What role should be played by developed versus developing nations in achieving global cyber security?
- How feasible is developing the metaverse considering the vulnerabilities and risks associated with it ?
- How the exploitation of blockchain technology can be grown into promising mitigation technology for cybersecurity?

BIBLIOGRAPHY

1. Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. Journal of Criminal Law and Criminology, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc
2. CERT India. (2009). Cyber Security & Role of Cert-In. https://www.itu.int/ITUD/cyb/events/2009/hyderabad/docs/rai-role-of-cert-in-sept-09.pdf
3. Council of Europe. (2001). Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
4. Developments in the field of information and telecommunications in the context of international security : https://www.un.org/disarmament/ict-security/
5. Cyber Capabilities and National Power: A Net Assessment", IISS, June 2021 : https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
6. "Cyberterrorism How Real Is the Threat?" United States Institute of peace : https://www.usip.org/sites/default/files/sr119.pdf
7. Fidler, M., & F. Madzingira. (2015, June 22). The African Union Cybersecurity Convention: A Missed Human Rights Opportunity. Council on Foreign Relations. https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity
8. Global Cyber Security Capacity Centre. (2017). Cybersecurity Capacity Portal https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front
9. "How The Vietnamese State Uses Cyber Troops to Shape Online Discourse", ISEAS,, March 2021: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong/
10. "Cyber Troops, Online Manipulation of Public Opinion and Co-optation of Indonesia's Cybersphere" : ISEAS, March 2022 : https://www.iseas.edu.sg/wp-content/uploads/2022/03/TRS7_22.pdf
11. "ICRC cyber-attack: Sharing our analysis", ICRC, february 2022 : https://www.icrc.org/en/document/icrc-cyber-attack-analysis
12. Lewis, J. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other CyberThreats. https://csis-prod.s3.amazonaws.com/s3fspublic/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
13. Madrid Guidelines Principles : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/448/85/PDF/N1544885.pdf?OpenElement
14. "Massive ransomware infection hits computers in 99 countries", BBC news 2017 : https://www.bbc.com/news/technology-39901382

15. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, S. Herzog, Journal of Strategy and security, 2011 : https://www.jstor.org/stable/26463926?seq=2
16. “Systemic Cyber Risk: A Primer”, Carnegie endowment, march 2022 : https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531
17. Sixth review of the UN Global Counter Terrorism Strategy : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/80/PDF/N1819880.pdf?OpenElement
18. “The story behind the Stuxnet virus”, Forbes, 2010 : https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html?sh=3ab6fa6a51e8
19. United Nations Counter Terrorism Office : Cybersecurity mandate : https://www.un.org/counterterrorism/cybersecurity
20. United Nations Office on Drugs and Crime, “The use of internet for terrorist purposes”, 2012 : https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
21. United Nations Office Office of Information and communication : https://unite.un.org/digitalbluehelmets/sites/unite.un.org.digitalbluehelmets/files/docs/digitalbluehelmets_brochure_final.pdf
22. United Nations Security Council Resolution 2341 (2017) : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/57/PDF/N1703857.pdf?OpenElement
23. “U.S. government and energy firms close ranks, fearing Russian cyberattacks, The Washington Post”, april 2022 : https://www.washingtonpost.com/national-security/2022/04/06/russia-cyber-attack-threat-energy/
24. “War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions”, Carnegie endowment, october 2020 : https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819

PIMUN

2022 !