SPRIMUN

SCIENCES PO RENNES INTERNATIONAL
MODEL UNITED NATIONS

STUDY GUIDE

UNITED NATIONS SECURITY COUNCIL

FOREWORDS

Distinguished delegates,

On the behalf of the 2022 organizing team, it is a pleasure to welcome you in Rennes for SPRIMUN. Along with the two chairs of this committee, Pauline Charpentier and David Baranowski, we hope that those three days of diplomacy will be full of success for you.

But most importantly, welcome to the Security Council, dear delegates, place of the harshest and strongest negotiations. You are reunited here to take decisions that could change the world's stability for ever.

The two topics you'll have to address require a high level of diplomacy; both are extremely challenging. A very careful preparation is needed not to bump into one of the many obstacles they present. Only keep one thing in mind: a resolution must be found!

Pauline and David have done an important work on this study guide, which gives you the opportunity to be perfectly ready for the conference. It gives you an overview of the main issues concerning the two topics and orients your researches in order to settle your country's position. Your position paper, and later, your speeches will have to reflect the information that you have been provided here.

To be successful in the committee and maybe even win awards, a careful preparation is needed, and includes a specific attention to this study guide. Two points are important in a MUN: your ability to represent the position of your designed country and, at the same time, your ability to work around this position in order to reach a fruitful compromise in the adopted resolution. Please keep in mind that it is strictly forbidden to bring already written draft resolutions to the conference, as all the working papers and draft resolutions should be only developed during SPRIMUN, not before.

Should you have any inquiry regarding the preparation of the conference, do not hesitate to contact us. We will do our best to make sure you live a great experience!

We wish you good luck in your preparation.

Best regards,

Flora Dano & Manon Delahaye
SPRIMUN 2022 Committees and Delegates Managers

Dear Delegates,

Welcome to the SPRIMUN and to the UN Security Council!I will try to accompany you from the best I can during this MUN, by being one of the two chairs of this committee.

I am currently in my fourth year of study in Sciences Po Rennes, and I am attending a Master's Program specialized in Security, Defense and Strategic Intelligence.

In February 2020 (just before the apocalypse), I participated in the MainMUN in Frankfurt, where I had the chance to represent Australia in the International Maritime Organization. It was an amazing opportunityto meet new people and to learn from other cultures, and I can not wait to participate in another MUN again. It will be my first time as official chair, but I will do my bestto apply conscientiously and rigorously the rules of procedure.

I hope that this study guide will help you in writing your position papers and I am very excited to meet you all in March in Rennes!

- Pauline Charpentier

Distinguished Delegates,

I am delighted to welcome you to SPRIMUN! My name is David Baranowski and I have the pleasure to be one of your chairs.

After three years of Political Science studies in Eichstätt (Germany) and Rennes, I am doing an internship in international project and event management in Paris at the moment and will complete my BA in philosophy this summer.

While this will be my first time as a chair, I have been part of very tight negotiations due to spectacular happenings in Main-MUN´s crisis committee in 2020. I am thrilled to be back in the MUN game, and I hope for great debates, diplomatic confrontations, and a good time together. Mayyour mission succeed.

I am looking forward to getting to know you soon!

Kind regards,

David Baranowski

How to use this study guide:

This document in not an exhaustive guide of the issues that will beraised regarding your committee's topics. The study guide provides guidelinesand references to help the delegates in doing their own research onthe issues.

UN SECURITY COUNCIL OVERVIEW

The United Nations Security Council was created in 1945, alongside with the organization itself. It is one of its most important committees and is generally considered as the "executive" power of the UN.

The Security Council comprises 5 permanent members, which have the right to veto any resolution. It also includes 10 non-permanent members, which are elected by theUnited Nations General Assembly, for a duration of two years. A 1991 resolution proposes a geographical distribution of these countries to ensure a certain equality among member states.

Permanent Members	Non-permanent Members
United States of America Russian Federation People's Republic of China United Kingdom of Great Britain and Northern Ireland France	Albania Brazil Gabon Ghana India Ireland Kenya Mexico Norway United Arab Emirates

The mission of the Security Council is to ensure peace all over the world. For this purpose, it adopts resolutions that are mandatory for each state, it imposes sanctions,and it can decide on military interventions. It also recommends a candidate for the position of Secretary-General of the United Nations, and it is involved in the process of nomination of the International Court of Justice judges.

TOPIC A:

THE SUPPLY OF WEAPONS TO TERRORISTS' GROUPS

INTRODUCTION TO THE TOPIC

- **Terrorism: definition & current situation**

It is very hard to find a universal and consensual definition of "terrorism" (which can, by the way, undermine the process of identifying and fighting this phenomenon). However, we can mention the definition present in the resolution 1566 of the General Assembly of the United Nations, from 2004, that refers to terrorism as:

> *"... criminal acts, including against civilians, committed with intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offenses within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature."*

In general, we can identify some common points to terrorists' groups:

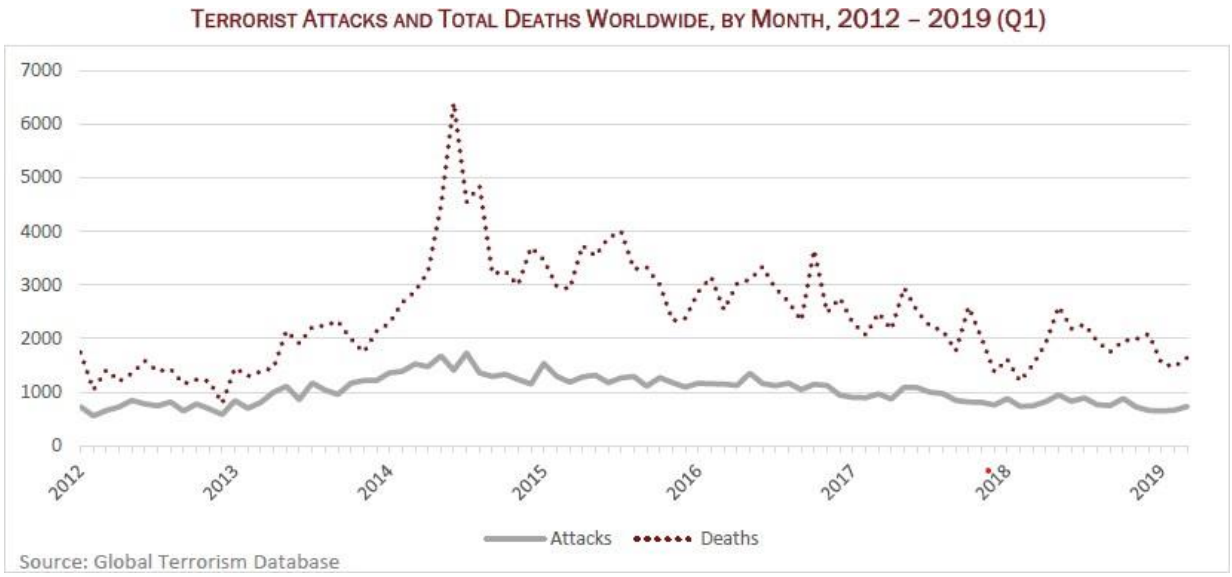
- the use of violence
- the will to spread fear and to coerce authorities into doing something
- the political aim

Terrorist attacks are generally the doing of non-state actors (ISIS, Al-Qaeda, ETA...), but state terrorism should not be dismissed, although it is much rarer. Terrorism is also often transnational, which explains the need of international cooperation in this area.

Terrorism is not a new phenomenon since the word exists at least since the 19th century. However, it has evolved a lot since then, following political transformations and technological progress. If terrorism was more related to ethno-nationalist and far-left groups from the 1970's to the 1990's, the 9/11 attacks put the Islamic terrorism at the center of the attention of many states. It concerns not only Western countries, but even more developing countries especially in the Middle East and in Africa. In 2018, one third of the attacks were perpetrated in Afghanistan (18%) and in Iraq (14%)[2]. The gravity of terrorist attacks is also not the same across time. We observed a peak of terrorist attacks in 2014, partly due to the power of ISIS at that time, but since then the frequency and scale of attacks are decreasing. Most victims are civilians.

[1] https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html

[2] https://www.start.umd.edu/gtd/trends-in-global-terrorism-islamic-states-decline-in-iraq-and-expanding-global-impact-fewer-mass-casualty-attacks-in-western-europe-number-of-attacks-in-the-united-states-highest-since-198/



- **Typology of weapons**

The supply of weapons to terrorists is a core issue in the fight against terrorism because it can have an impact on the scale and the frequency of attacks. One needs to separate conventional weapons from weapons of mass destruction (WMD).

- Conventional weapons[3]: they are the most common and historically the most used for terrorist attacks. It can refer to weapons themselves (machine guns, rifles, grenades…) but also to ammunition and to vehicles. They are subject to restrictionsby international law ("arms control") and some are even forbidden due to their grave impact (such as mines). Small Arms and Light Weapons (SALW) are more difficultto control and to contain for authorities.

- Weapons of Mass Destruction (WMD)[4]: refer to the CRNB weapons (chemical, radiological, nuclear and biological weapons). Since 9/11, it has been crucial for moststates to contain the spread of such weapons considering their natural dangerousness. In contrast to conventional weapons, WMD are totally forbidden,and that is the relevant expression is "disarmament" and not "arms control". The only exceptions are the nuclear weapons developed by the 5 permanent members of the Security Council. WMD are very seldom used by terrorist groups, because they are really difficult to produce, to acquire and to master for non-state actors.

HISTORIC APPROACH: CASE STUDIES

How did terrorists' groups get their weapons for these major attacks?

- Tokyo's subway attack (20/03/1995)[5]: in 1995, the "Aum Shinrikyo" cult perpetrated a sarin gas attack in Tokyo's subway, that resulted in the death of 13 people and in the injury of 5,500 others. It is one of the rare examples of a chemical terrorist attack. The chemicals were produced in large quantities by scientists of the groups. However,this attack could have been even more damaging because the substance was not used at its full capacity, making it less dangerous.

[3]https://www.un.org/disarmament/conventional-arms/
[4]https://www.un.org/disarmament/wmd/
[5]https://www.britannica.com/event/Tokyo-subway-attack-of-1995

- 9/11: on September 11th, 2001, the USA suffered from a massive terrorist attack perpetrated by Al Qaeda, whose most famous illustration is the crash of deviated airplanes into the towers of the World Trade Center. This attack caused the death of nearly 3,000 people. It showed the USA and the world that vehicles such as airplanes could be used as weapons, and it led to the reinforcement of controls in strategic infrastructures (airports, harbors, train stations…). More generally, it also prompted a "war against terror", with multiple military interventions in the Middle East and with a strengthening of arms controls throughout the world.

- Paris attacks (13/11/2015): in 2015, Paris and its surroundings underwent coordinated attacks led by ISIS fighters, that caused more than a hundred deaths. The main weapons used are Kalashnikov assault rifles, explosive belts, and vests (conventional weapons). This series of attacks proved the limits of arms controls in Europe, since many of these weapons were smuggled into Europe, through the Balkans especially[6]. The recent attacks in Europe showed that terrorists groups tend to return to conventional weapons, whereas there was more diversity in the past.

TREATIES, CONFERENCES & CONCRETE SOLUTIONS

Ever since the rise of the terrorist peril, countries have tried to fight this phenomenon by multiple means and canals. It is one of the most tackled issues at the UN (whether we speak of the General Assembly or of the Security Council), and the agreements and resolutions are quite numerous. That is why we will not suggest an exhaustive list on the topic, but we will try to highlight the main documents.

- Biological Weapons Convention, adopted in 1972 and entered into force in 1975[7]: this convention forbids the development, production, use… of biological weapons. It is addressed to anyone (states, groups, etc).

- Chemical Weapons Convention, adopted in 1992 and entered into force in 1997[8]: this convention forbids the development, production, use… of chemical weapons. It is addressed to anyone (states, groups, etc). The Organization for the Prohibition of Chemical Weapons was created in 1997 to apply the text of the convention.

- Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition (Firearms Protocol): adopted by a resolution of the UNGA in 2001 and entered into force in 2005. This protocol aims to control arms trafficking.

- UN Security Council resolution 1373 (2001): this resolution was adopted after the 9/11 attacks and exhorts states not to support terrorist groups by supplying them with weapons, and to implement tougher controls on arms.

- Program of Action on small arms and its International Tracing Instrument [9]: international agreements respectively adopted in 2001 and 2005, to propose a better regulation of small arms and light weapons. They are not legally binding.

- UN Security Council resolution 1540 (2004)[10]: this resolution forbids states to provide assistance in any form whatsoever to terrorists' groups to acquire weapons. The 1540 committee was created to ensure the implementation of this resolution.

[6] https://time.com/how-europes-terrorists-get-their-guns/
[7] https://www.un.org/disarmament/biological-weapons
[8] https://www.un.org/disarmament/wmd/chemical/
[9] https://www.un.org/disarmament/convarms/salw/programme-of-action/
[10] https://www.un.org/disarmament/wmd/sc1540/

- Arms Trade Treaty[11]: adopted in 2013 by the UN General Assembly and entered into force in 2014. This treaty created a framework to regulate arms trade on a global scale.

- UN Security Council resolution 2370 (2017): this resolution tackles specifically the question of the supply of weapons to terrorists' groups. It enjoined states to respect the arms embargoes currently implemented and to fight effectively against arms trafficking. Particular attention is paid to small arms and light weapons.

PRINCIPAL POSITIONS

The supply of weapons to terrorists' groups is quite a consensual topic among members of the Security Council, and in general resolutions on this matter are unanimously voted.

- **USA/UK/France**

The United States of America, the United Kingdom and France are traditionally very proactive regarding to fighting terrorism, because they have experienced some major attacks in the past years. For example, the Arms Trade Treaty is the result of a French-British initiative (among others).

- **The Russian Federation**

The Russian Federation is also determined to prevent terrorists to acquire weapons. However, Russia did not sign the Arms Trade Treaty.

- **People's Republic of China**

Ever since the beginning of this century, the PRC has been more and more proactive in the fight against terrorism. It is part of all major international agreements relating to this issue, including the ATT. The PRC is also becoming more involved in the UN peacekeeping forces.

GUIDING QUESTIONS

- How to contain the supply of weapons to terrorists' groups by States?
- How to contain the acquisition of weapons by terrorists' groups from transnational organized crime entities?
- How to prevent the production of weapons by terrorists' groups?
- How to contain the spread of Weapons of Mass Destruction (WMD)?
- How to fight against the trafficking of small arms and light weapons?
- How to enforce arms embargoes?

LINKS AND USEFUL SOURCES

Please refer to footnotes.

[11] https://www.un.org/disarmament/convarms/att/

TOPIC B:
PREVENTING THE RISE OF CYBER-ATTACKS

INTRODUCTION TO THE TOPIC

The digital world is developing very fast and offers uncountable opportunities, butit also creates new vulnerabilities. Many states invested in building critical infrastructure in the cyberspace and rely on computer-based systems for stocking top secret information. Nonetheless, the world wide web is a border free space andas such, it is also a space for diverse crimes. The topic is even more significant intimes of pandemic policies when work, shopping and social life mainly happen in cyberspace.

As a consequence, many states agree that security measures need to be adapted in order to protect their citizens, especially in the banking sector, and their own national infrastructures.

"Cyberattack" is the general term regrouping all kinds of attempts "to gain illegal access to a computer system for the purpose of causing damage or harm."[12] These may include stealing, copying, manipulating, or deleting critical information from the victim´s computer or network. There are different techniques to do so:

a) Hacking: The hackers access a network without the permission of its owner.Some would just leave a trace that they were there without actually doing something, other would search for specific information and possibly manipulate or steal it.[13]

b) Spreading malware: This includes sending viruses to or installing viruses on the victim´s computer or network. It may not only give the attacker unauthorized access to critical information, but also disturb the functionsof the attacked computer or network.[14]

c) Phishing: This is a technique based on identity fraud and theft. The attacker uses a wrong identity and asks the victim to provide him or herwith critical information, for example passwords.[15]

[12] See Merriem/ Webster: Dictionary, 2022. URL: www.merriam-webster.com/dictionary/cyberattack.
[13] See: Farlex: The Legal Dictionary, 2022. URL: legal-dictionary.thefreedictionary.com/hacking.
[14] See American Heritage Dictionary of the English Language. Malware. 2016. In: ibid. URL: www.thefreedictionary.com/malware.
[15] See Embree, Mary (ed.): Abused, Confused, & Misused Words. Phishing. 2007, 2013. In: ibid, phishing. URL: www.thefreedictionary.com/phishing.

d) Denial of Service attack: The attacker sends a huge amount of data to the attacked server in order to overload it. Consequently, it will stop working for a certain amount of time, but not destroy the system.[16]

Cyberattacks take place regularly and target all kinds of institutions. For instance, hackers breached into UN systems in spring 2021.[17] On a state level, cyberattacks may affect political and important infrastructural domains. But they may also be a tool for certain purposes, especially for the access to critical information concerning potentially dangerous groups, individuals, or other states. Cyberspace is also a place for general cyber warfare and espionage, and it is not always easy to detect criminal activity in cyberspace. Additionally, if detected it is often relatively difficult to determine who is responsible for a cyberattack, and who gave the orders the attacker followed.[18]

Even though most states are very conscious of the security risks of cyberspace, several actors underline the lack of UN cooperation in the field. While some states cooperate with each other, there is no specialized UN organization for cybersecurity, and no binding international framework that would help to punish cybercrime. Nonetheless, the United Nations´ Office of Counterterrorism and the United Nations´ Office of Information and Communications Technology treat relevant issues.[19]

TREATIES, CONFERENCES AND CONCRETE SOLUTIONS

The first major treaty on cybersecurity was the so-called "Budapest Convention", signed in 2001. It has 66 parties today, most of them European states and allies of the so-called West. 14 further states are signatories and invited to accede.[20] For the signing states, the Budapest Convention is a landmark in the field. It namely states that international law is applicable on the world wide web. Nevertheless, in its aftermath legal measures stay executed by states principally; in fact, the convention contains a set of crimes recommended to be punished by national law, including for instance child pornography (Art. 9), copyright frauds (Art. 10), and unauthorized

[16] See The Computer Language Company: Denial of Service Attack, 2019. In: Farlex: The Legal Dictionary. URL: encyclopedia2.thefreedictionary.com/Denial+of+service+attack.

[17] See Lyngaas, Sean; Roth, Richard: United Nations confirms hackers breached its systems earlier this year. In: CNN, 9/9/2021. URL: edition.cnn.com/2021/09/09/politics/junited-nations-cyberattack-april/index.html.

[18] See United Nations´ Security Council: Resolution 73/27. New York City, 2018, paragraph 1.1.2.

[19] See United Nations´ Office of Counter-Terrorism: Cybersecurity. Online, 2022. URL: www.un.org/counterterrorism/cybersecurity and United Nations´ Office of Information and Communications Technology. Online, 2022. URL: unite.un.org/information-security.

[20] See Council of Europe: The Budapest Convention and its Protocols. Budapest, 2001. URL: www.coe.int/en/web/cybercrime/the-budapest-convention#{%%22:[0]}.

preservation of data (Art. 16-17). It is also lying the base for mutual assistance amongthe parties in fighting cybercriminal activities (Art. 25).[21]

Since then, different institutions have worked on cybersecurity, and several have published more recent guidelines for national legislations. These institutions include Interpol, ENISA, the NATO, and the OECD.

While there is no detailed and binding legal UN framework, several resolutions have been adopted by the UN Security Council. These include the following:

55/63; 56/121 (2001/02, condemning the misuse of information technologies),
64/211 (2010, giving practical advice and guidelines for a "global culture of cybersecurity").
68/243; 69/28; 71/28 (2013/14/16, deciding to continue talks on informationsecurity, relying to a group of governmental experts)
73/27 (2018, agreeing to continue cooperation, forcing member states to meet their obligations and respect human rights on the internet,establishing an open-ended working group on information security withregular meetings)

PRINCIPAL POSITIONS

Almost all states regularly signal their general support for fighting cyber-attacks.The listed resolutions would not have been possible without a certain consensus. Nonetheless, the interpretation of the existing framework seems different from stateto state. If you as a government hack a terrorist´s network, is it illegal? Who is a terrorist and who is not? What exactly is "misuse" of information and communication technology? What do "harm" and "damage" mean in cyberspace? Who decides on these questions? After all, there is often no other place than the UN Security Council to address such highly politized topics, and there have been a lot of discrepancies on these questions in specific conflicts, especially between the UN Security Council´spermanent members, who can veto against any resolution in their disfavor.

All states show themselves ready to cooperate, but have national concerns, especiallywhen it comes to sharing too much information on their own cybersecurity systems. The permanent members´ positions are as follows (in alphabetical order):

21 See: Council of Europe: Convention on Cybercrime. Budapest, 2001. URL: rm.coe.int/1680081561.

French Republic / United Kingdom of Great Britain and Northern Ireland:
Both are parties of the Budapest convention.[20] They are convinced that international law and human rights are applicable on the web. Both states would wish to punish states that break the established rules and recommendations and strengthen international cooperation on the issue. In cooperation with the USA and NATO, they have condemned PRC´s "malicious cyber activities" in 2021.[22] Both states are ready to hold talks with all actors, but ask for binding and concrete commitments, especially by the Russian Federation.[23]

United States of America: In the USA, cybersecurity is part of national security, especially since several US-experts accused Russian hackers of influencing the political campaigns before 2017 US elections. In 2021, they condemned PRC´scriminal activity on the internet, joined by NATO and the EU.[22] The USA support the Paris Call for Trust and Security in Cyberspace of 2018 and wish to cooperate in the field in order to better punish cyberattacks. [24] PRC´s officials hold the USA responsible for cyberattacks against them. [25] The USA are parties of the Budapest Convention.[20]

People´s Republic of China: The PRC has not signed the Budapest Convention,[20] but wishes to continue international cybersecurity cooperation. Accused of conducting harming activities in cyberspace, including hacking, it denies any responsibility for criminal acts stating that these acts were conducted by individuals for personal financial benefits, and not by the PRC itself. According to official statements, the PRC is a victim of attacks by the USA itself.[25]

Russian Federation: The Russian federation has not signed the Budapest Convention.[20] Regularly, different (mostly Western) states accuse hackers with links to Moscow to attack its networks, most recently the USA in 2021,[26 but] also Ukraine, for instance, in January 2022.[27] Russia is also suspected to be behind the first major cyberattack against another state, Estonia, in 2007. These attacks are still a key reference in the sector.[28] Moscow does not admit any fault of their part and announced it would actively try to strengthen cooperation in the field with the European Union in December 2021.[23]

---

[22] See: The White House: The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People´s Republic of China. In: The White House: Statements and Releases, 9/7/2021. URL: www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[23] See Reuters: Russia proposes holding collective cybersecurity talks with EU-TASS. 16/12/2021. URL: www.reuters.com/technology/russia-proposes-holding-collective-cybersecurity-talks-with-eu-tass-2021- 12-16/.

[24] See Jones, David: US backs Paris-led effort on cybersecurity cooperation. In: Cybersecurity Dive, 11/11/2021. URL: www.cybersecuritydive.com/news/us-paris-cybersecurity-cooperation/609905/.

[25] See Feng, Emily; Martinez, A.: China Denies Cyberattacks Accusations, and Says it too is a Victim of Hacking. in: NPR, 20/7/2021. URL: www.npr.org/2021/07/20/1018271511/china-denies-cyberattack-accusations-and-says-it-too-is-a-victim-of-hacking?t=1642673260963.

[26] See Crane, Emily: Russian hackers targeting US networks in ´very large and ongoing´ cyberattack. In: New York Post, 25/10/2021. URL: nypost.com/2021/10/25/russian-hackers-target-us-networks-in-ongoing-cyberattack/.

GUIDING QUESTIONS

1. What can the UN Security Council do to make the digital world a safer place?
2. How can your nation´s cybersecurity be ensured in a globalized world, in whichone can launch a cyberattack from everywhere?
3. What can the UN Security Council do to prevent cyberattacks against states?
4. What can the UN Security Council do to prevent cyberattacks against majoractors of the private sector?
5. What can the UN Security Council do to punish cyberattacks?
6. Should the states exchange their knowledge on cybersecurity to protect themselves better?
7. Would your government support a binding legal framework on cybersecurityat UN-level?
8. If yes, how could it be implemented?

LINKS AND USEFUL SOURCES

Council of Europe: The Budapest Convention and its Protocols. Budapest, 2001. URL: www.coe.int/en/web/cybercrime/the-budapest-convention#{%%22:[0]}.

→ a list with all parties of the convention and general information

Council of Europe: Convention on Cybercrime. Budapest, 2001. URL: https://rm.coe.int/1680081561.

→ full text of the Budapest Convention

United Nations´ Office of Counter-Terrorism: Cybersecurity. Online, 2022. URL: www.un.org/counterterrorism/cybersecurity.

→ some words on the misuse of information and communication technology and cyberterrorism

United Nations´ Office of Information and Communications Technology. Online, 2022. URL: unite.un.org/information-security.

→ information on the United Nations´ cybersecurity manager

United Nations´ Security Council: Resolution 73/27. New York City, 2018. URL: undocs.org/A/RES/73/27.

→ the most recent important resolution on cyber-attacks

Refer also to footnotes.

---

[27] See Dilanian, Ken; De Luce, Dan; Reuters: Ukraine hit by cyberattack, Russia moves more troops after talks hit ´dead end´. In: NBC News, 14/01/2022. URL: www.nbcnews.com/news/world/ukraine-cyberattack-russia-troops-nato-talks-invasion-rcna12203.

[28] See Software Engineer Training: The Cyber-Attacks in Estonia, August 2007. Online, 12/5/2012. URL: software-engineer-training.com/the-cyber-attacks-in-estonia-august-2007/.

We are looking forward to the debates!

See you soon in Rennes, Brittany!

Kind regards,
Pauline Charpentier and David Baranowski