Background Guide

United Nations Office of Counter Terrorism

AlexMUN 2023

President : Valentina Appendini

Moderator : Gustavo Oliva

Conference Officer : Luciano Alcocer

Index

I. **Presentation**

Hello, and welcome delegates, my name is Valentina Appendini and I will be your president of the UN office of Counter Terrorism. This years we will be addressing recent conflicts regarding the rise of cybercrime against marginalized groups and hate crimes against the muslim LGBTQ+ community. If you have any doubts about anything, you can contact me via email; valentina.appendini@bab.edu.mx

Hi delegates, my name is Gustavo Oliva and I will be serving as your moderator in the committee of UN office of Counter Terrorism. If you have any issue regarding the topics we will be addressing or anything else, you can contact me via email; gustavo.oliva@bab.edu.mx

Hello, my name is Luciano Alcocer and I will be your conference officer in the committee of UN office of Counter Terrorism. I look forward in working with all of you, so if you have any questions feel free to contact me via email; luciano.alcocer@bab.edu.mx

II. Introduction

The United Nations Office of Counter Terrorism (also known as UNOCT), was established on June 15, 2017 by Mr. Vladimir Voronkov. The creation of this Office, is considered the first major institutional reform carried out by the UN Secretary General, António Guterres. Because UNOCT provides secretariat support, this Office works together with the members of United Nations Global Counter-Terrorism Coordination Compact in order to prevent and counter terrorism and the underlying spread of violent extremism.

On September 8th, 2006, the UN General Assembly approved the UN Global Counter-Terrorism Strategy. This strategy, is a special global tool to strengthen regional, international, and national counterterrorism activities.

It is important to mention, that the Counter Terrorism Office has come main functions **(Faculties)**

- To take the lead in the General Assembly in implementing the Secretary General's anti-terrorism directives for the entire UN system.
- To increase the Global Counter Terrorism Coordination Pact's coherence and coordination.
- To fortify the provision of the UN assistance to create counter terrorism capacity of the Member states, as well as to improve the visibility, advocacy, and mobilization of resources for United Nations counterterrorism efforts
- To ensure that the fight against terrorism is given the required priority throughout the entire United Nations system, and as it is important to remember that preventing violent extremism is embedded on Strategy

The new Global Counter Terrorism Coordination Pact of the United Nations was signed by the Secretary-General on February 3, 2018.

The pact intends to strengthen a common-action strategy for coordinating the operations of the UN system in the fight against terrorism and the prevention of violent extremism (CPVE). Additionally, it seeks to improve the assistance provided to Member States in carrying out pertinent United Nations resolutions and mandates, including the Global Counter Terrorism Strategy, upon their request.

The United Nations Counter Terrorism Center (UNCCT), which was established in 2011, helps Member States strengthen their capacity via counterterrorism initiatives and activities all across the world.

UCCT Projects and Programs:

- Cybersecurity = The goal of the Cybersecurity and New Technologies Program is to improve Member States' abilities to stop and reduce the abuse of technology advancements. With a mandate to improve Member States' ability to prevent and respond to terrorist attacks, UNOCT collaborates with Security Council subsidiary groups such the Counter Terrorism Committee

- Engaging parliamentarians = Through this program, UNOCT assists parliaments all over the world in their efforts to combat terrorism and stop violent extremism. Their work is founded in the implementation of the UN Global Counter Terrorism Strategy

- Terrorist travel = This program improves Member States' capacity to identify, follow, and stop terrorists' travels. It marks a crucial improvement in the UN system's coordination and coherence in the fight against terrorism

- Sports and security = Through this program, they promote sports and their core principles as a vital weapon in the fight against radicalization and the violent extremism that leads to terrorism

- Border security = In this program, border officers' abilities are improved while helping countries incorporate such practices into their national policies and action plans to combat terrorism

The UNOCT is composed of 15 delegations in total:

1. People's Republic of China
2. Republic of Estonia
3. Republic of France
4. Republic of India
5. Republic of Ireland
6. Republic of Kenya
7. United Mexican States
8. Federal Republic of Nigeria
9. Kingdom of Norway
10. Russian Federation
11. Saint Vincent and the Grenadines
12. Republic of Tunisia
13. United Kingdom of Great Britain and the Northern Ireland
14. United States of America
15. Socialist Republic of Vietnam

Topic A: The rise of cybercrime against marginalized groups

Cybercrime is a criminal activity that either targets or uses a computer, a computer network or a networked device. The majority of cybercrime is conducted by hackers or cybercriminals who are for financial gain. However, there are times when cybercrime aims to harm computers or networks for factors other than financial gain. These might be either personal or political.

Threats to cyber security have grown around the globe in recent years. As businesses shifted to remote working environments during the pandemic, cybercriminals profited from misaligned networks. Compared to 2019, malware assaults climbed by 358% in 2020. From then, the number of cyberattacks increased by 125% globally through 2021, and through 2022 and 2023, an increasing number of cyberattacks continued to put businesses and individuals at risk.

Historical context:

The way in which cybercrime has been presented throughout history has been changing over the years. Two thieves obtained access to the financial markets in 1834 by hacking the French telegraph system and stealing information. Many experts believe that this incident was the first cybercrime, which was then followed by various cybercrimes that each targeted newly developed technology.

With the internet development all over the world, the 1990s gave rise to some of the finest communication technologies known to mankind, but the news weren’t all positive. These developments led to a rise in cybercrime. Hackers and other bad actors took advantage of the fact that trust and safety measures weren't initially a key priority when these new technologies were being created and implemented.

The primary focus of these early days was developing ground-breaking apps for communications and commercial efficiency because cybersecurity was not a name nor an active field. Nevertheless, a shadow economy was steadily gaining power.

Here is a little timeline of the most important cybercrime events that had happened trough our history.

Cybercrime during the 1990's:

- 1994 = A "password sniffer" application was used by Datastream Cowboy and Kuji (a 16-year-old British student and his accomplice), to carry out a series of attacks that damaged the Air Force's Rome Laboratory while obtaining research data that was used as attack instructions for jets in battle.
- 1998 = Under false pretenses, Max Butler, a security expert who worked for the FBI broke into websites run by the US government. Officials were made aware of his crimes by the US Air Force, and he was given an 18-month term. Later, he received a record-breaking 13-year sentence for a hacker for yet another illegal venture.

Cybercrime during the 2000's:

- 2008 = Heartland Payment systems were targeted using a mix of SQL injection, password sniffers, and malware in one of the worst intrusions ever, exposing the data of 134 million people.

Cybercrime during the 2010's:

- 2010 = The Stuxnet worm, labeled the first "digital weapon" in history, targeted Iranian nuclear sites and destroyed the nation's uranium enrichment capabilities. Also, Chinese military hackers conducted Operation Aurora against more than 20 top technological businesses When Google informed the public that some of its intellectual property had been taken in the assault, the people learned about the attacks.

- 2016 = The Austrian Aerospace firm, lost 50 million Euros due that finance employees were tricked to transfer this money into bank accounts controlled by cybercriminals. As a result, the company's CEO was fired.
- 2017 = WannaCry, probably the most sophisticated ransomware variant managed to infect more than 200,000 Windows PCs across 150 countries. Given that the UK's National Health Service Hospitals were among the most severely damaged, it was particularly dangerous and devastating. It is largely believed that North Korean hackers were responsible for the attack.

Cybercrime during 2020's:

- 2020 = In one of the most devastating hacking incidents of 2020, foreign intelligence agents used a compromised SolarWinds program to break into approximately 18,000 personal and government-affiliated systems. Russian cyberattacks on U.S. government organizations appear to be on the rise. A wealth of personally identifiable information, including financial data, source code, usernames, and passwords, were made available to cybercriminals as a result of these data breaches.

Nowadays, recent studies led by Marcin Kleczynski (CEO of Malwarebytes) have shown that minorities like women, black people, Asian communities, and in general, minorities, carry an increased burden when talking about the consequences of cybercrime. In the interview, 35% of women said they didn't feel safe online and 53% said they were afraid of their personal data to be exposed or used.

It is important to mention that some specific groups of people (according to Robert Burda, Interim Chief Executive Officer at Cybercrime Support Network) , tend to be at greater risk online depending on the sort of cybercrime. It can be said that more women than men receive texts from unknown numbers or users that can contain potentially harmful links. By the other hand, more black and indigenous experience social media account hacks people compared to white people. Also it has been proved that the risk of having credit card information stolen increases with age, with individuals 65 and older being more affected than any other age group.

Finally, “The Demographics of Cybercrime” (presented by Malwarebytes in partnership with Digitunity) show that 76% of people have received texts from unknown users, 29% had their credit hard hacked, 42% had their social media accounts hacked, and 17% had their identity stolen.

For more static regarding your specific country, you can check the next link: https://aag-it.com/the-latest-cyber-crime-statistics/

Relevant International action:

The “Internet Governance Forum” is celebrated every year to adres internet related issues.

In 2019, the General assembly adopted a resolution called “countering the use of information and communication technologies for criminal purposes”, and started working on a new international treaty on cybercrime that can establish global policies in order to protect human rights.

The sessions in the creation of this treaty have been going on for three years. The first meeting took place in march 2022, however the treaty has not been finished.

The next session will take place in Vienna, where this topics will be addressed:

- Kinetic cyber-attacks to critical infrastructure and/or IoT devices
- Spread of terrorist content online
- Online terrorist communications
- Digital terrorist financing

Here are some UN documents regarding cybercrime and cybersecurity:

- 6th review of the UN Global Counter-Terrorism Strategy A/RES/72/284
- UN Security Council Resolution 2341 (2017)
- UN Security Council Resolution 2370 (2017)

- Security Council text S/2015/939 (Madrid guiding principles)

Countries/Organizations directly involved:

1. People's Republic of China
2. Republic of Estonia
3. Republic of France
4. Republic of India
5. Republic of Ireland
6. Republic of Kenya
7. United Mexican States
8. Federal Republic of Nigeria
9. Kingdom of Norway
10. Russian Federation
11. Saint Vincent and the Grenadines
12. Republic of Tunisia
13. United Kingdom of Great Britain and the Northern Ireland
14. United States of America
15. Socialist Republic of Vietnam

Analysis:

Cybercrime is a problem that although it's not generally recognized as something serious, it is, and it has become more common and frequent nowadays because of the technological growth and development. Even though cybercrime can affect and threat a whole country, it can also directly influence the lives of marginalized groups (like women, black communities, old people, LGBTQ+ communities, etc).

For all states of the UN, it is important to guarantee a safe cyberspace, so everyone can feel safe and free to use it without any threat. Numbers regarding cyberattacks on marginalized groups have been increasing through the past years (this can be due to multiple factors, including the pandemic).

Possible solutions:

1. Countries must prioritize granting cybersecurity to its population, they must create different national or international strategies in order to guarantee security and freedom on the cyberspace, and to do this, they must establish some legal regulations in order to control the internet. Talking specifically about marginalized groups, government should focus on this people and provide help and online security (since it has been proven that they are a target in cyberattacks)

2. Nowadays the use of biometrics is part of almost all technological devices, however sometimes they are used in an incorrect way. Usually biometrics should be stored in only one device, however if they are stored in on a server, this information is vulnerable and could be compromised. By doing this, cyberattacks agains marginalized groups could decrease.

3. Educate vulnerable people (specially people that belong to marginalized groups), so they know and prevent cyberattacks. Crucial information that could help them avoid a cyberattack will be given, for example: avoid giving personal information online, avoid responding or opening links from unknown numbers, etc. and the way they must react if sadly they are facing this kind of situation.

4. Promote and give free antivirus tools in order to prevent cyberattacks on marginalized groups and other people.

Conclusion:

Cybersecurity is a topic that must be addressed in order to reduce cyberattacks globally. Nowadays people do not feel safe on the internet due that cyberspace isn’t secure. It has been shown how cyberattacks can come in many forms and can happen to anybody, however, marginalized groups or minorities are an important part of our community that is principally being affected by this problem. Now that government are starting to understand the importance of addressing this problem, the United Nations Office of Counter Terrorism is searching for ways to solve this situation so millions of people feel safe and free to use the cyberspace again without being threatened.

Topic B: Hate crimes against the Muslim LGBTQ+ community

People that are part of the LGBTQ+ community (lesbian, gay, bisexual, transgender, queer, intersex people, among others) are routinely exposed to discrimination or hate crimes due to their sexual orientation. In the case of muslim people that are part of this community, they must deal with this type of attitudes from the world, but also from their religion. Muslim people who are part of the LGBTQ+ community sadly live realities where their integrity and life are put at risk due to hate crimes they have to experience in their daily lives.

Historical context:

The Muslim world and perception of the LGBTQ+ community has been influences by its social, political, religious, cultural and legal history. Muslims believe in the *Quaran* (sacred scripture of Islam), and on it, homosexual activity is prohibited and condemned with death penalty. Islam societies have recognized "both erotic attraction and sexual behavior between members of the same sex", however they often show discordant attitudes about them.

Here is a little timeline of the most important cybercrime events that had happened trough our history.

Pre-modern era:

- There is small evidence of homosexual practice in Islamic communities, however, homoerotic poetry starts to appear at the end of the 8th century (in Baghdad on the works of the poet Abu Nuwas)
- Around 809, due to the increase of homosexual thoughts in the Islamic communities, the two holy cities of Mecca and Medina declared this type of behavior as a "corruption of morals"
- The concepts of homosexuality that are found on classic texts of Islam, are similar to the ones ancient Rome and Greece wrote, causing that didn't have the modern understanding of sexual orientation

Modern era:

- In 1744, Muhammad bin Saud (ruler of Diriyah) dedicated his next seventy years to establish a state that followed the true Islamic principals, and because of this, homosexuality (which had been accepted during the Ottoman Empire) was criminalized and punished with dead.
- In 1979 during the Islamic Revolution, hundreds of political opponent were killed and got justified by accusing them of homosexuality.
- In 1991, homosexuality became a capital offense in Iran's Islamic Penal Code
- In 2005, 2006, and 2016 there was evidence tat people were hanged because of homosexual behavior (however execution grounds in Iran are really difficult to track, since if you are not part of the Islamic community you can't enter to certain places)
- In some countries like Egypt, homosexual behavior is not explicitly criminalized, however people that are part of the LGBTQ+ community are prosecuted under vague "morality laws" of the country
- Due to the rule of Abdel Fattah el-Sisi, arrests and hate crimes towards the LGBTQ+ community have increased

Laws in Muslim countries

- According to the ILGA (International Lesbian and Gay Association), 7 countries have capital punishment for homosexual behavior, which are: Saudi Arabia, Iran, Afghanistan (has death penalty since 2021 since the Taliban takeover), Mauritania, Northern Nigeria, and United Arab Emirates.
- In Algeria, Qatar, Uzbekistan, and the Maldives, homosexuality is punished with prison or a fine.
- In Egypt, homosexual people have been prosecuted due to "morality laws"
- The Sunni Islamist militant group and Salafi-jihadist terrorist organization (which invaded parts of Iraq and Syria between 2014 and 2017), have declared a political and religious persecution of LGBTQ+ people and decreed capital punishment
- In India (third largest muslim population worldwide) since 2018 homosexuality is no longer considered a criminal act

- In Iran (according to its article 129 and 131), homosexual people can received up to 100 lashes of whip or death penalty

Relevant International action:

The 25 of November, 1981, a document called “Declaration on the elimination of all forms of intolerance and discrimination based on religion or belief” was made by United Nations in order to protect individuals from different hate actitudes which were justified by a religion or specific belief.

The document can be found on the next link: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/406/81/IMG/NR040681.pdf?OpenElement

The United Nations has also created a document called “UN Strategy and Plan of Action on Hate Speech”, where different strategies or actions are proposed when dealing with hate actitudes.

The document can be found on the next link: https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf

Also in September, 2015, international and globally recognized organizations like: UNODC, UN WOMEN, UNESCO, ILO, UNDP, World Health Organization, WFP, UNAIDS, among other, created a document where the violence and discrimination against the LGBTQ+ community was discussed.

The document can be found on the next link: https://www.ohchr.org/sites/default/files/Documents/Issues/Discrimination/Joint_LGBTI_Statement_ENG.PDF

Countries/Organizations directly involved:

1. People's Republic of China
2. Republic of Estonia
3. Republic of France
4. Republic of India
5. Republic of Ireland
6. Republic of Kenya
7. United Mexican States
8. Federal Republic of Nigeria
9. Kingdom of Norway
10. Russian Federation
11. Saint Vincent and the Grenadines
12. Republic of Tunisia
13. United Kingdom of Great Britain and the Northern Ireland
14. United States of America
15. Socialist Republic of Vietnam

Analysis:

Globally, people belonging to the LGBTQ+ community live realities where they are discriminated, assaulted, and attacked for the simple fact of being part of this community. For people who are part of the Muslim community, being part of the LGBTQ+ community carries a greater risk because it is penalized with prison, physical assaults (such as whipping), or even the death penalty since it is something that is considered "prohibited" in their religion.

This causes homosexual, bisexual, etc., people to have to live in fear and in realities where their integrity and life are in danger, where they do not have freedom of expression, speech, or thought.

Possible solutions:

Because it is impossible to change the Islamic religion and what it says about people who are part of the LGBTQ+ community, you can ask to help people who live these realities so that they can have a better life.

1. Countries neighboring Islamic areas should receive Muslim refugees who are part of the LGBTQ+ community who are persecuted by their country and give them the opportunity to have a better quality of life.

2. The United Nations and countries belonging to them should speak with the leaders of Islamic countries to guarantee fair treatment for gay, lesbian, bisexual, etc. people, in order to end these attacks and hateful attitudes that Islamic countries have

3. Since these attitudes on the part of Islamic countries have existed for a long time, it is difficult to generate a quick and effective change, however, the United Nations could start by seeking to remove the death penalty in Islamic countries for homosexual conduct.

Conclusion:

Muslim people who are lesbian, gay, bisexual, transgender, queer, intersex people, among others, have very difficult realities that they must face every day, however, their human rights are violated through an extremely vague justification where depriving a person of their freedom of thought, expression, among other things, is correct in the eyes of countries belonging to Islam.

Bibliography

- Terrorism committee UN. (n.d.). *Security Council. Counter Terrorism Committee*. Retrieved from: https://www.un.org/securitycouncil/ctc/ç

- United Nations. (2021). *Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats*. Retrieved from: https://press.un.org/en/2021/sc14563.doc.htm

- Kenyon, T. (2021). *Cybercrime is impacting communities differently, study finds.* Retrieved from: https://cybermagazine.com/cyber-security/cybercrime-impacting-communities-differently-study-finds

- Arctic Wolf. (2022). *A Brief History of Cybercrime.* Retrieved from: https://arcticwolf.com/resources/blog/decade-of-cybercrime/

- United Nations. Office of Counter Terrorism. (2017). *UN anti-crime agency at 20; tackling terrorism, cybercrime vital for peaceful and sustainable future.* Retrieved from: https://www.un.org/counterterrorism/events/un-anti-crime-agency-20-tackling-terrorism-cybercrime-vital-peaceful-and-sustainable-future

- Malwarebytes. (n.d.). *Demographics of Cybercrime Report.* Retrieved from: https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html

- United Nations. Office of Counter Terrorism. (n.d.). *Cybersecurity.* Retrieved from: https://www.un.org/counterterrorism/cybersecurity

- AAG. (2023). *The Latest 2023 Cyber Crime Statistics.* Retrieved from: https://aag-it.com/the-latest-cyber-crime-statistics/

- United Nations. (n.d.) *Islamophobia*. Retrieved from: https://www.un.org/en/observances/anti-islamophobia-day

- Wikipedia. (2022). *LGBT people and Islam.* Retrieved from: https://en.wikipedia.org/wiki/LGBT_people_and_Islam#Modern_laws_in_Muslim-majority_countries

- United Nations. (n.d.) *Hate speech*. Retrieved from: https://www.un.org/en/hate-speech/impact-and-prevention/targets-of-hate

- United Nations. (n.d.). *Use of religious beliefs to justify rights violations must be outlawed says UN expert.* Retrieved from: https://news.un.org/en/story/2020/03/1058411