TOPIC GUIDE

DISEC

The Disarmament and International Security Committee

Index 1

Letter from the Presidents

Regards honorable delegates,

On behalf of the Disarmament and International Security Committee (DISEC), it is our great pleasure to welcome you to this year's conference.

We are pleased to welcome you to the twelfth version of SAMUN. Our names are Mariana Calume and Daniela Pizarro and this year we will be presiding over the Disarmament and International Security committee.

As this is our first time presiding in a model, we are particularly honored to have the opportunity to lead and facilitate the discussions that will take place over the course of the conference. We recognize the responsibility that comes with this role and we are committed to ensuring that this year's conference is a productive and memorable experience for all.

Throughout the conference, we will be discussing a range of important topics related to global security, such as weapons proliferation, disarmament, and arms control. We believe that these issues are critical to promoting peace and stability, and we look forward to hearing the perspectives and insights that each and every one of you will bring to the table. We believe that through our collective efforts and cooperation, we can identify solutions to some of the most pressing issues related to disarmament and international security.

We encourage you to actively participate in the discussions, engage in constructive and respectful dialogue, and work towards finding common ground on the issues at hand. As this is a learning experience for all of us, we also welcome any feedback or suggestions that you may have for us.

Once again, we are delighted to welcome you to this year's conference, and we look forward to working with each and every one of you.

If you have any doubt or restlessness don't think it twice before contacting us
samun.disec@cbsm.edu.co
Sincerely,
Mariana Calume & Daniela Pizarro
DISEC presidents

Introduction to DISEC

The Disarmament and Security Council (DISEC) is the First Committee of the United Nations General Assembly, established in 1945. DISEC accompanies main bodies that report to it, the Disarmament Commission (UNDC) and the Conference on Disarmament (CD). The committee ensures problems regarding the “disarmament, global challenges and threats of peace that have an effect on the global community, seeking resolutions to the challenges that this problem carries out within the international security regime.”

Within DISEC a few landmark resolutions have been made, including the first General Assembly resolution “Establishment of a Commission to Deal with the Problems Raised by the discovery of Atomic Energy" in 1946, additionally, DISEC had passed the first General Assembly resolution that was co-sponsored by all the Member States at the time. Later on, this resolution was adopted in 2001, which reaffirmed the resolutions on the situation involving Afghanistan and confirmed that the United Nations would play an important role in this country. Regardless, the resolutions passed by this committee are non-binding resolutions and are formatted as recommendations to the nations that make up this committee.

Furthermore, given its direct association with the United Nations General Assembly (being a subsidiary organ as authorized 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. This includes providing recommendations to the Members of the United Nations or to the Security Council, discussing any questions raging the maintenance of international peace and security.

Topic A: The illegal possession and arm trading of small arms and light weapons

Key Concepts:

Arm trading: The arms trade is the trade in weaponry and other military and security equipment. Governments buy arms from their own national industries and/or others, and sometimes one country gives arms away to another.

Illegal Market: An illegal market is an economic activity that occurs outside of government-sanctioned channels. Underground markets trade in illegal goods and services, legal goods and services to avoid taxes or both.

Small Arms/Light Weapons: Small arms are weapons designed for personal use, including light machine guns, sub-machine guns, machine pistols, fully automatic rifles and assault rifles, and semi-automatic rifles.

Global Security: Global security includes military and diplomatic measures that nations and international organizations such as the United Nations and NATO take to ensure mutual safety and security.

Illicit Manufacturing: Illicit manufacturing means the manufacturing or assembly of firearms, their parts and components or ammunition: from parts and components illicitly trafficked, without a license or authorization from a competent authority of the State party

where the manufacture or assembly takes place, or without marking the firearms at the time of manufacture, in accordance with article 8 of the Firearms Protocol.

ATT: The Arms Trade Treaty (ATT) is an international treaty that regulates international trade in conventional arms and seeks to prevent and eradicate illicit trade and diversion of conventional arms by establishing international standards governing arms transfers. The Treaty came into force on 24 December 2014. At this stage, the Treaty has a total of 112 States Parties and 29 States that have signed but not yet ratified the Treaty.

Weapons proliferation: Weapons proliferation refers to the spread of weapons, to states or non-state actors that do not possess them or have the capability to produce them. This is a major concern for international security, as it can destabilize regions, increase the likelihood of armed conflict, and pose a serious threat to global peace and stability. It is often associated with the illegal trade and trafficking of arms, as well as the failure of states to adequately secure and regulate their weapons stockpiles.

Introduction

The illegal trade in small arms and light weapons is a crucial problem which contributes to conflict, crime, and human rights abuses. This trade is carried out frequently by non-state actors such as organized crime groups and armed militias, and it often occurs in countries with weak governance and security systems.. It often happens through illicit channels, the sale and transportation of these weapons, such as the black market, and they are repeatedly trafficked across borders. International organizations and governments have implemented various measures such as arms embargoes, arms trade treaties, and border control measures to combat this problem.

Small arms and light weapons (SALW) are a major contributor to violence, conflict, and insecurity around the world. The illegal trade in these weapons refers to the transfer of firearms, ammunition, and other related materials that is unauthorized, unregulated, or prohibited by national or international law. The illegal trade in SALW is driven by a range of factors, including weak firearms regulations, conflict, poverty, and organized crime.

The illegal trade in SALW has a wide-ranging impact on global security, fueling armed conflicts, exacerbating crime and violence, and undermining peace and stability in many regions. The consequences of the illegal SALW trade can also be felt at the local level, with communities affected by increased crime and violence, and individuals facing greater risks to their personal safety.

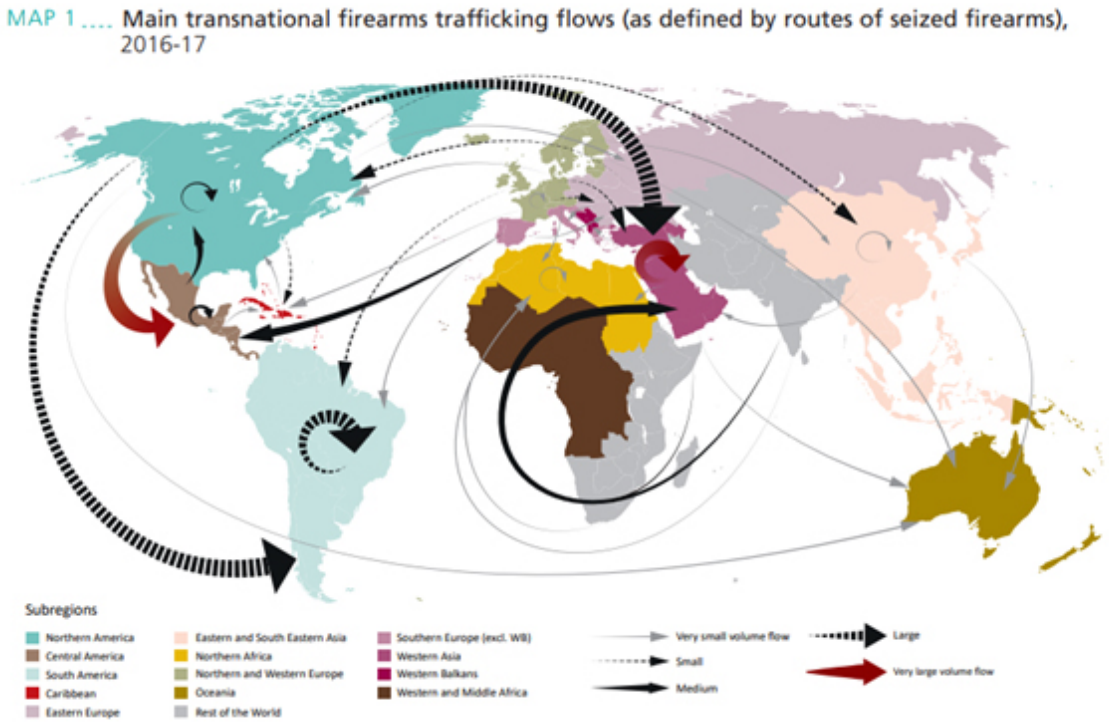
Efforts to combat the illegal trade in SALW typically focus on strengthening national and international regulations, disrupting trafficking networks, and improving international cooperation to prevent the illicit flow of these weapons across borders.

Current Situation and Approach

The black market arms trade refers to the illegal trade in firearms and weapons that occurs outside of government oversight and regulation. These transactions are typically conducted through underground networks and black market dealers, and the weapons traded can include both legal and illegal firearms. The black market arms trade is driven by demand from individuals and groups who are unable or unwilling to obtain weapons through legal channels, as well as by profits from the illegal sale of weapons.

The black market arms trade is a major concern for governments and law enforcement agencies around the world, as it contributes to violence, crime, and instability. Efforts to combat the black market arms trade typically focus on disrupting illegal arms trafficking networks, cracking down on illegal weapons sales, and strengthening laws and regulations to make it more difficult for criminals to obtain and trade illegal firearms.

The sale of illicit arms on the dark web refers to the illegal trade of firearms and weapons through encrypted and anonymous online marketplaces. These transactions typically occur on dark web platforms that cannot be accessed through conventional search engines and require specialized software or authorization to access. The anonymity of the dark web makes it a popular destination for individuals seeking to purchase illegal arms without attracting law enforcement attention.



Many illegal arms are trafficked from conflict zones, corrupt officials, and criminal networks in countries such as Afghanistan, Iraq, Somalia, and Syria. In other cases, arms are illegally

manufactured and sold within a country's borders, such as in the case of underground firearms production in countries like Brazil, Mexico, and the Philippines. Countries involved in the illicit trade of arms both as suppliers and as transit points for weapons destined for other countries. The illegal arms trade can have serious consequences for regional stability, security, and human rights. Countries that are considered sources of illegal arms include the United States, Russia, China, and some European countries such as Belgium and the Czech Republic. Major destinations for illegal arms include Mexico, Afghanistan, Somalia, and Yemen.

Russia is one of the major producers and exporters of conventional weapons and military equipment, and its arms industry is a significant contributor to the country's economy. However, there have also been reports of illegal arms trafficking from Russia, with some of these weapons ending up in the hands of criminal organizations, insurgent groups, and terrorists.

The Russian government has taken steps to prevent illegal arms trafficking, but the problem persists. The ease with which weapons can be obtained in Russia, along with its porous borders, make the country a major source of illegal arms that are trafficked across the world. The illegal arms trade from Russia often involves organized criminal groups and can fuel conflict, crime, and instability in regions where these weapons end up.

International laws regulating the possession of weapons vary, but some international agreements address the issue, such as the United Nations Arms Trade Treaty (ATT) which came into force in December 2014. The ATT aims to regulate the international trade in conventional arms and prevent the transfer of arms if they are likely to be used for human

rights abuses or violations of international humanitarian law. However, not all countries have signed or ratified the treaty, and its implementation can vary from country to country.

Additionally, regional agreements and national laws also play a role in regulating the possession of weapons. Some countries have strict gun control laws, while others have more relaxed laws that allow for widespread private ownership of firearms. It is important to note that the laws and regulations regarding the possession of weapons can change, so it is always best to check the most current information for a specific country.

Regional organizations such as the European Union and the Organization of American States also have agreements in place to regulate the transfer of weapons within their regions. However, these regulations are often limited to member states, and their implementation and enforcement also face challenges.

QARMAS

- Has your country been involved in arms trading? If this is the case, in which way has it been?
- What measures the nation is planning to implement to avoid illegal arms trading?
- What kind of sanctions is the country willing to have to avoid the problem?
- Is your country willing to have international approval for the legal possession of weapons?
- Is it appropriate for their citizens to have access to purchase illegal weapons as a form of self-defense?
- Has your country signed treaties and/or protocols proposed by the United Nations against illegal arms trading? If yes, which ones?

- Are government agencies in your country raising awareness of illegal arms trading?

Questions

- What are the root causes of the illegal possession and arms trading of small arms and light weapons, and how can they be addressed?
- Should the international community prioritize stricter regulations on the trade and possession of small arms and light weapons?
- How can we ensure that small arms and light weapons do not end up in the hands of non-state actors or terrorist groups?
- What role can technology play in preventing the illegal trade of small arms and light weapons, such as through improved tracking and identification systems?
- Should there be more international cooperation and coordination among countries to prevent the illegal trade of small arms and light weapons?
- How can we balance the need for individuals and states to possess small arms and light weapons for self-defense with the need to prevent their illegal trade and possession?
- How can we address the issue of illicit manufacturing of small arms and light weapons, which often fuels their illegal trade and possession?
- Should there be more strict background checks and licensing requirements for individuals and businesses involved in the trade and possession of small arms and light weapons?
- Does your country benefit economically from this market?
- Is your country affected by this issue? If yes, in which way?

Useful Links

- https://www.youtube.com/watch?v=CH9bjhCEbiI
- https://www.youtube.com/watch?v=6cbemozTeb4
- https://www.youtube.com/watch?v=6LmPq7D-ds0

Topic B: Addressing the implementation of espionage and counter-intelligence by government officials in foreign countries

Key Concepts

Espionage: the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company

Counter-Intelligence: : Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Cybersecurity: Cybersecurity involves tools, services, systems, and best practices designed to help with the detection, prevention, and mitigation of crime that involves the internet. There are common types of cyberattacks that Cybersecurity aims to address, including phishing, malware, ransomware, and cyberterrorism.

Classified Information: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf

of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities

Counterespionage: That aspect of CI designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities

OPSEC: A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.

DDoS attacks: DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

Spear-phishing: Spear-phishing is a type of phishing attack that targets specific individuals or organizations typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware.

Introduction

Threats to the global community posed by foreign intelligence entities are becoming more complex, diverse, and harmful to universal interests. Foreign intelligence actors—nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure, and steal sensitive information, research, technology, and industrial secrets. They are conducting malicious influence campaigns using cyber operations, media manipulation, covert operations, and political subversion to sow divisions in our society, undermine confidence in our democratic institutions, and weaken our alliances. Foreign threat actors have become more dangerous because, with ready access to advanced technology, they are threatening a broader range of targets at lower risk.

Espionage focuses on gathering non-public information through covert means. Classified information is kept secret in the first place because its disclosure might harm national security, jeopardize the country's economic well-being, or damage international relations. Its sensitivity makes it necessary for us to protect it but also makes it attractive to spies.

If this information is obtained by those with no right to access it, serious damage can be caused. For instance, other countries are seeking technical details of weapons systems so that they can find ways of neutralizing our military advantages. Information on key services such as gas, oil and transport could enable terrorists to seriously damage these important economic targets. And the theft of classified technologies could enable foreign companies to copy them, threatening both national security and jobs.

Counter intelligence is conducted in three overlapping phases: detection, or the recognition of some actual or apparent evidence of subversive activity; investigation, or finding out more

about this evidence; and research and analysis, which puts the information into such order that some use may be made of it. Detection techniques include surveillance; publicity (citizens made aware of the danger of subversive activities); and liaison, through which counter-intelligence agencies are afforded each other's cooperation and that of other public and private security agencies so as to maximize their range of observation for evidence of subversive activity or legal subversion.

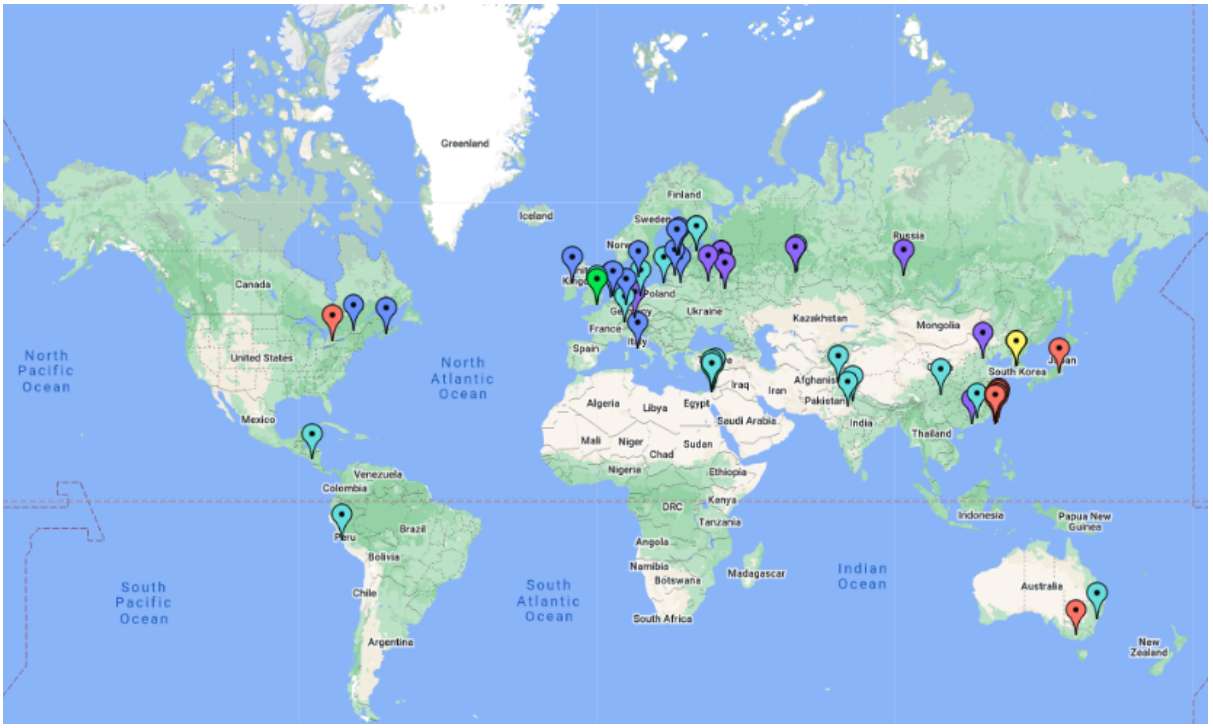
Current Situation and Approach

Numerous countries and organizations fall victim to various types of cyber attacks. Many of these attacks were attributed to state-sponsored hacking groups, with several countries being blamed for the attacks, such as Russia, China, Iran, and North Korea. The types of attacks included DDoS attacks, spear phishing, malware deployment, data breaches, data theft, and disinformation campaigns. The targets of these attacks included government institutions, media companies, defense firms, energy companies, blockchain platforms, political parties, and even social media accounts. The consequences of these attacks varied, ranging from temporary website disruptions to the theft of sensitive data and financial losses.

The attacks have targeted government agencies, defense and high tech companies, and have caused significant losses. The attacks have used various methods such as ransomware, phishing, and malware to obtain sensitive information and disrupt services. The attacks have been carried out against countries in Europe, Asia, and the Americas, highlighting the global nature of the threat. The timeline highlights the need for constant vigilance and preparedness against the ever-evolving threat of cyber attacks.

The threat of cyber attacks is constantly evolving and it is important for organizations and countries to stay vigilant and prepared. The best way to do this is by implementing strong cybersecurity measures, such as regular software updates, employee training programs, and implementing multi-factor authentication. Additionally, organizations and countries should also regularly review their cybersecurity protocols and make changes to their systems to stay ahead of the latest threats. It is also important to establish a robust incident response plan to quickly address any security incidents that may occur.

this map would provide a visual representation of the global distribution of international espionage operations, highlighting the countries responsible for directing the operations and the countries targeted by the operations. It could be a valuable tool for analyzing and understanding trends in international espionage over the past decade.



https://www.google.com/maps/d/viewer?mid=1mXn9vQxihxhyqx7QnRvL6t28yf8&hl=en_US&ll=33.30183872157603%2C41.411530434183305&z=2

In addition to these measures, international cooperation and information sharing is also essential in combating cyber attacks. By sharing information on the latest threats and methods used by hackers, organizations and countries can work together to protect against future attacks. This can also lead to more effective law enforcement action against those responsible for the attacks.

It is widely acknowledged that intelligence services of many countries, including France and China, have been involved in collecting economic intelligence to support their domestic businesses. However, the methods used by these intelligence services can range from legitimate activities such as gathering information on infrastructure and resources to more controversial practices.

It's important to note that while most countries do use their intelligence services to aid their private businesses, this doesn't necessarily mean that they are stealing trade secrets and intellectual property from foreign firms. However, some countries do engage in such practices, which raises questions about the actions of the intelligence services. The use of intelligence services for economic purposes is a complex issue and can range from legitimate to unethical practices, depending on the country and the methods used.

QARMAs

- Has your country been involved in the unethical practices of this problematic, if this is the case, how do you intend to convince other delegations to understand the reasoning behind these actions?

- Should countries be involved in unauthorized espionage practices? And if so, how?
- How essential is the posture of a country in this conflict?
- How is the classified information obtained by other countries weaponized?

Questions

- What are the consequences that occur, when countries find it necessary to breach the confidentiality that exists within the global community?
- Has espionage and counterintelligence affect the transparency within the global community?
- Does counterintelligence hold an effect in the rise of cyber attacks that has taken place in the last decades?
- How does espionage tactic benefit countries that participate in these actions?
- Is there any way to ensure the safe recollection of data among countries, without causing discord among the global community?
- How is your country involved and affected with this problem?

Useful Links

- **https://www.fbi.gov/investigate/counterintelligence/the-china-threat**
- **https://www.mi5.gov.uk/counter-espionage**
- **https://www.sciencedirect.com/topics/social-sciences/espionage**
- **https://www.usatoday.com/story/news/politics/2022/08/12/what-is-the-espionage-act/10312311002/**
- **https://www.gov.uk/government/publications/national-security-bill-factsheets/espionage-etc-national-security-bill-factsheet**