INTERPOL

Lyon Model United Nations 2017
Study Guide

Welcome Letter

A warm welcome to the delegates of the Interpol committee at LyonMUN 2017!

We are delighted to chair this committee at this leading French MUN conference, and have been working together to provide you delegates with two of the most interesting topics an Interpol simulation has ever seen!
First of all, it is a real chance to be a part of this committee that is rarely featured. Delegating within the Interpol is a different experience as you will focus on that specific region instead of a global issue. And it is symbolic to be a part of it within LyonMUN, seeing that the headquarters of the organisation are located here.
You will get the chance to explore two major issues that are not dealt with often at MUN conferences :   dealing with the return of ISIS soldiers from Syria and Iraq and tackling cybercriminality. The first one is a specific political problem that most countries are facing, as you delegates will focus on a definite area : the countries that are affected by the return of their citizens that joined ISIS, and how to tackle the threat they represent. It is a crucial topic to deal with as numerous casualties occurred and instability has become the normal stance. The second topic features a larger amount of countries and people, as cyber criminality can affect numerous populations across the continent.
 In both cases, millions of persons are facing those issues.
It is of the highest importance, more than ever, to tackle them.
We are providing you with a detailed study guide, and I expect all of you to use the information well. It is meant to help you find subtopics, especially for the Moderated Caucuses, as well as prove as a direction for the committee to follow. The resolutions can only be complete and efficient if you study all fields that can be examined. We advise you to not only stick to the sources coming from the actual Interpol , but also to study those from UN committees (DISEC, SPECPOL, UNSC), regional bodies (especially the EU subcommittees), NGOs, and to follow the daily news dealing with the featured topics. Never hesitate in checking varied media to discover the different approaches to deal with the topics.

If the organisation we are simulating has been criticized throughout the previous years, it is clearly engaging in an ambitious way to making the world more peaceful. It is up to you to find the most creative solutions to the featured problems. We are very excited to see what you will make of our Interpol!

Should you have any questions regarding the committee and its topics, the position papers or any of our expectations concerning the preparation and the debates, don’t hesitate to contact us, either via our email addresses or through the social media! Looking forward to heated debates and a great time in Lyon!

Best regards,

Florian Guidat, Director
Chahnaz Lagha, Assistant Director

II- INTRODUCTION TO THE COMMITTEE[1]

INTERPOL, International Criminal Police Organization, is the world's largest international police organization, with 190 member countries. The role is to enable police around the world to work together to make the world a safer place. Our high-tech infrastructure of technical and operational support helps meet the growing challenges of fighting crime in the 21st century.

The idea of establishing an international police cooperation organisation emerged at the first International Criminal Police Congress in 1914, which was held in Monaco. During these sessions, lawyers, policemen and magistrates from 24 different countries met to discuss different procedures and technologies related to the capturing of criminals. Officially created in 1923 as the International Criminal Police Commission with headquarters in Vienna, Austria, on the initiative of Dr Johannes Schober, president of the Vienna Police., the Organization became known as INTERPOL in 1956.

Supporting police worldwide

INTERPOL works to ensure that police around the world have access to the tools and services necessary to do their jobs effectively. We provide targeted training, expert investigative support, relevant data and secure communications channels.

This combined framework helps police on the ground understand crime trends, analyse information, conduct operations and, ultimately, arrest as many criminals as possible.

Neutrality

INTERPOL aims to facilitate international police cooperation even where diplomatic relations do not exist between particular countries. It is imperative to recognize that Interpol itself is not a police force; never in its history has an Interpol employee made an arrest, and it never will. The focus of Interpol is to facilitate quick, secure communication between police forces and to protect the sovereignty of each of its member nations. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. Our Constitution prohibits ‘any intervention or activities of a political, military, religious or racial character'.

A global presence

The General Secretariat is located in Lyon, France, and operates 24 hours a day, 365 days a year. INTERPOL also has seven regional offices across the world and a representative office at the United Nations in New York and at the European Union in Brussels. Each of our member countries maintains a National Central Bureau staffed by its own highly trained law enforcement officials. Buenos Aires is home to Interpol’s Americas based Command and Coordination Center (CCC), the central hub for police communications in the Americas region. There is a similar CCC for Europe, Asia, and Africa at Interpol Headquarters. Interpol’s Global Complex for Innovation, located in Singapore, is a cutting-edge research facility dedicated to the improvement and modernization of policing techniques around the world. Interpol’s locations and programs are funded primarily by member dues, which are determined by a country’s economic output. Additional contributions by countries and other groups are made on a voluntary basis.

The Vision: "Connecting police for a safer world"

The Mission: "Preventing and fighting crime through enhanced cooperation and innovation on police and security matters"

INTERPOL Notice System[2]

At LyonMUN, you will be able to use notices (similar to directives in crisis committees) as a mini-crisis will take place during the committee

Within Interpol’s data sharing network, countries share Notices: color-coded, universally understood warnings or calls for action sent to pertinent member countries and relevant bodies.

- Red notice: “To seek the location and arrest of a person wanted by a judicial jurisdiction or an international tribunal with a view to his/her extradition”
- Blue notice: “To locate, identify or obtain information on a person of interest in a criminal investigation.”
- Green notice: “To warn about a person’s criminal activities if that person is considered to be a possible threat to public safety.”
- Yellow notice: To locate a missing person or to identify a person unable to identify himself/herself.
- Black notice: “To seek information on unidentified bodies.”
- Orange: “To warn of an event, a person, an object or a process representing an imminent threat and danger to persons or property.”
- Purple: “To provide information on modi operandi, procedures, objects, devices or hiding places used by criminals.”

Partnership with the United Nations[3]

The UN and Interpol signed an official, overarching cooperation agreement in 1997 that detailed the areas in which they were to cooperate, particularly in the taking down of transnational crime and the promotion of world safety. More recently, Interpol has entered into specific cooperation agreements with different committees, offices, and departments of the United Nations, with a focus on enforcing sanctions and bolstering peacekeeping operations.

The General Assembly[4]

At LyonMUN, the Committee will meet as the General Assembly.

The General Assembly is composed of delegates appointed by the governments of member countries. As INTERPOL's supreme governing body, it meets once a year and takes all the major decisions affecting general policy, the resources needed for international cooperation, working methods, finances and programmes of activities.

The General Assembly also elects the Organization's Executive Committee. Generally speaking, the Assembly takes decisions by a simple majority in the form of Resolutions. Each member country represented has one vote.

TOPIC A: MANAGING THE RETURN FROM ISIS SOLDIERS FROM IRAQ AND SYRIA

The phenomenon

Increasingly, we are seeing ISIS works to radicalize individuals and inciting them to leave their homes to become foreign terrorist fighters. This group leverage the Internet and social media for recruitment, creating a truly global security threat.

Individuals – often young people – are being lured from communities worldwide to travel to conflict zones in the Middle East to join ISIS operating primarily in Iraq and Syria, and increasingly in Libya. These individuals sometimes use fraudulent identity documents to reach their destinations undetected. Those who return to their countries of origin pose even greater security risks, as they can exploit the military skills they learned abroad to carry out attacks on their home territory.

All the more complicated, their return may be due to different reasons, whether it is a reintegration and a return to normal, or the continuity of their acts in their territory of origin. Since these reasons are never perfectly clear, the distinction between a person seeking reintegration and another seeking destruction is very difficult to do and the police forces in each country find themselves with a choice to make: to aim for rehabilitation and to face At the risk that an agent of chaos will pass through the cracks, or enclose the largest number and polarize opinion against the internal forces of the country. Despite its emphasis on the return of combatants, the situation of "civilians" must be taken into account, as prolonged questioning of these could serve as an example of government oppression used by The EI.

In the face of such a formidable and increasingly widespread common enemy, the cohesion of the international police force is absolutely crucial. INTERPOL provides the world with an arena of discussion in order to establish concrete solutions against a force of international evil. This arena of discussion also allows the exchange of information and intelligence in order to identify leaders or cells of the Islamic State traveling from one country to another. Prevention and identification work will enable INTERPOL to further contain the expansion of radicalism, eliminate attacks and work towards the reconversion and reintegration of returning combatants.

Origins of ISIS soldiers

In December 2015, The Souphan Group released its second 'Foreign Fighters in Syria' report[1]. The Soufan Group has calculated that between 27,000 and 31,000 people have traveled to Syria and Iraq to join the Islamic State and other violent extremist groups from at least 86 countries. The top 5 foreign fighters nationalities are Tunisia (around 6000 soldiers), Saudi Arabia (around 2500), Russia (2400), Turkey (2100) and Jordan (2000). The Middle East provides around 8240 soldiers, in front of th Maghreb (8000) and Western Europe (5000). Concerning Europe, '3,700 of the total 5,000+ European Union foreign fighter contingent come from just four countries': France, the United Kingdom, Germany and Belgium.

Travel

There are several access roads to the Islamic State, notably by countries bordering Syria and Iraq like Turkey. The journey is now often fragmented for future jihadists with numerous arrests as well as the illegal crossing of borders often through corruption. The many border security measures taken by governments have drastically changed the roads of fighters who often combine aircraft, boat and car. Turkey is the largest area of access to Syria. Once in Syria, the fighters join the town of Raqqa where is the headquarters of the Islamic State. For the fighters coming from Europe, America or Asia, the simplest mode of transport is the plane. To be detected, the fighters make several journeys before arriving in Turkey: they are 'fragmented flights'. With the Schengen laws, all members with a European passport can cross the borders of the European Union without control. This is problematic for European police forces because it is therefore difficult to control the borders within Europe when it comes to track down the path of Islamist fighters. With increasingly high aviation security, jihadists are struggling to avoid being spotted by the authorities. So some prefer the land or sea route to reach Syria, often from Europe or North Africa. The most common route is the Balkans, as far as Bulgaria and from there, access to Turkey. Greece is also a transit point. Concerning the African

[1] For information: http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate_FINAL3.pdf

region, the most common point of convergence for Turkey is Libya, as well as Tunisia.

The United Nations

The 24th September 2014, the United Nations Security Council unanimously adopts Resolution 2178 on "Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters"[5]. This resolution recognizes INTERPOL's global role against the threat posed by foreign terrorist fighters. stipulates that:

"*Noting* with appreciation the efforts of INTERPOL to address the threat posed by foreign terrorist fighters, including through global law enforcement information sharing enabled by the use of its secure communications network, databases, and system of advisory notices, procedures to track stolen, forged identity papers and travel documents, and INTERPOL's counter-terrorism fora and foreign terrorist fighter programme,"

13. *Encourages* Interpol to intensify its efforts with respect to the foreign terrorist fighter threat and to recommend or put in place additional resources to support and encourage national, regional and international measures to monitor and prevent the transit of foreign terrorist fighters, such as expanding the use of INTERPOL Special Notices to include foreign terrorist fighters;"

Counter-terrorism tools

- Special notices[6]

The INTERPOL-United Nations Security Council Special Notice is issued for individuals and entities that are subject to sanctions imposed by the United Nations Security Council. Its principal function is to alert national law enforcement authorities that certain sanctions apply to designated individuals and entities. The three most common sanctions are:

- Assets freeze: freezing funds or other assets. There is no requirement to seize or confiscate assets;

- Travel ban: preventing an individual from entering or transiting through territories. There is no requirement to arrest or prosecute these individuals;
- Arms embargo: preventing the direct or indirect supply, sale or transfer of arms and related materials.

The Special Notice was created in 2005, as a way to combine the UN sanctions regime with INTERPOL's well-established notice system into an effective law enforcement tool.

Of course, classic notices (as described in the section 'Introduction to the Committee') can be used.

- INTERPOL Incident Response Team (IRT)[7]

In the event of a terrorist attack, member countries may request the assistance of an INTERPOL Incident Response Team (IRT). Experts can be quickly deployed to the site of the incident to provide a range of investigative and analytical support services, in coordination with the General Secretariat. An INTERPOL Incident Response Team (IRT) is deployed at the request of a member country during a crisis situation. The teams promote cooperation among countries and facilitate access to INTERPOL's tools and services.

There are two types of IRT:

- Disaster – an emergency response to unforeseen catastrophic events, such as large-scale accidents or natural disasters;
- Crime – the deployment of specialized personnel to assist and support a member country faced with a major or serious police issue. Crime IRTs provide specific expertise and investigative support to police.

An IRT can be briefed, equipped and deployed anywhere in the world within 12 to 24 hours of an incident.

- Data exchange[8]

As national boundaries become increasingly meaningless to criminals, effective and timely police communication across borders is more important than ever before. At

INTERPOL, one of our priorities is to enable the world's police to exchange information securely and rapidly.

INTERPOL offers a number of tools and services to help member countries enhance security at their borders, and works with national authorities to extend access to its I-24/7 secure communications network to border points to ensure these tools are accessible on the frontlines.

Three databases are crucial to these border management efforts:

- Nominal database
- Stolen and Lost Travel Documents database[9]
- Travel Documents Associated with Notices.

Police cooperation is important, but also co-operation in the legal field and in justice. The exchange of information has resulted in numerous arrests and is a valuable aid in the prevention of terrorist attacks. It is thus beneficial for all countries to share their information relating to the Islamic State. Border control, especially in Turkey and Syria and Iraq, is crucial to avert the influx of Islamic fighters. The UN Security Council is calling on the international community to strengthen Interpol's capabilities and to develop border security assistance and its communication networks, as well as to work more on the 'Stolen and Lost Travel Documents database'.

Counter-Terrorism Fusion Centre

INTERPOL's Counter-Terrorism Fusion Centre (CTF) investigates the organizational hierarchies, training, financing, methods and motives of terrorist groups.

In particular, Project Foreign Terrorist Fighters has been set up to address the issue of individuals who travel to a country that is not their own, for the purpose of planning, preparing or participating in terrorist acts, especially in conflict zones, and the threat to other countries after their training in these conflict zones.

The CTF's activities are global in scope and implemented through a number of regionally focused but interlinked projects. The aim is to improve the exchange of law enforcement information across borders and to enrich law enforcement practices.

- Project Al Qabdah (Middle East and North Africa);
- Project Amazon (Americas);
- Project Baobab (Africa);
- Project Kalkan (Central Asia);
- Project Nexus (Europe);
- Project Pacific (Southeast Asia and Pacific Islands).

Other major projects focus on:

- Terrorist use of social media and the internet;
- Hostage-taking for ransom.

Best example of cooperation: EUROPOL and European Counter Terrorism Centre (ECTC)[2]

Against this background the need has become apparent for an effective response to terrorism through enhanced cross-border cooperation between relevant counter-terrorist authorities. To this end, Europol's European Counter Terrorism Centre (ECTC) officially started operations on 1 January 2016. The ECTC focuses on:

- Tackling foreign fighters;
- Sharing intelligence and expertise on terrorism financing (through the Terrorist Finance Tracking Programme and the Financial Intelligence Unit);
- Online terrorist propaganda and extremism (through the EU Internet Referral Unit);
- Illegal arms trafficking;
- International cooperation among counter terrorism authorities.

However, this model of cooperation is obviously possible thanks to the existence of a great political and economic union, the European Union. For some countries, giving this kind of confidential information can be seen as a loss of sovereignty. It is

[2] For more information:
https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc
https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism

therefore necessary to strike a balance at the international level to meet the requirements of all member-states.

Case studies

The success of rapid information sharing is clear. In December 2014, three individuals – two men aged 18 and 27, and a 15-year-old boy – wanted in Spain on terrorism-related charges were arrested in Bulgaria at a border checkpoint with Turkey, just hours after INTERPOL issued an alert. They were believed to be heading to join insurgents in Syria. Another individual wanted for terrorist offences was apprehended in Lebanon on his way to Syria in October 2014, thanks to Belgium's decision to issue an international alert through INTERPOL.

Key elements a resolution should address

- Cooperation and the exchange of information between countries and the member states' police are crucial to resolving the problem of returning combatants
- Online recruitment of Islamic fighters must be monitored
- A census of combatants is necessary and must be accessible to all member states
- Identify funding for the recruitment and travel to the Middle East of combatants
- Determine individuals killed in combat
- Track the return of trained individuals in Syria
- Identify the different routes and modes of communication used
- Constant update of no-fly lists
- The danger of local attacks after the return of fighters

To follow the latest INTERPOL's press release regarding INTERPOL's meetings/works on terrorism please follow this link:
https://www.interpol.int/Crime-areas/Terrorism/Events

[1] For more informations: https://www.interpol.int/About-INTERPOL/Overview

[2] For more information :
http://www.interpol.int/en/News-and-media/Publications2/Fact-sheets/International-Notices-system/

[3] For more information:
https://www.interpol.int/About-INTERPOL/International-partners/United-Nations

https://www.interpol.int/en/News-and-media/Publications2/Leaflets-and-brochures/Cooperation-between-INTERPOL-and-the-UNITED-NATIONS-Security-Council/

[4] For more information :
https://www.interpol.int/About-INTERPOL/Structure-and-governance/Introduction

[5] For more information :
https://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf

[6] For more information :
https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices

[7] For more information :
https://www.interpol.int/INTERPOL-expertise/Response-teams

[8] For more information :
https://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7

[9] For more information :
https://www.interpol.int/INTERPOL-expertise/Border-management/SLTD-Database

Topic B : Tackling Cybercriminality

What is Cybercriminality ?

As much as technology made spaces tighter and exchanges easier, it can be a real threat to peace and stability. Of course, it helped bettering the world, but also increased what is called the cybercriminality. This criminal area is growing and expanding as technology advances.

Cybercrime, also known as « computer related crime », is a type of crime that is more and more used by criminals. It involves the use of telecommunications networks and a device such as a computer or a mobile phone. Cybercrimes intentionally harm the victims. Copyright infringement, hacking and child pornography can be mentioned as types of cybercrimes.

It is important to bear in mind that both states non-state actors are concerned by cybercrimes and even engage in this crime. This involved unwarranted mass-surveillance, espionage, governmental devices hacking, banks theft, money transfer to criminal organisations and so on. At least $445 billion are lost every year due to cybercrimes. Cybercrime is a real threat to world's peace, seeing the heavy damage it causes, especially those linked to finance, innovation and market trade, by hacking business plans and ideas.

In 2014, Russia has lost $3.99 M, Japan $6.91M and the United States $12.6 due to cyberhacking.

The internet and technology in general being speed, accessible, convenient and sometimes anonymous, hacking and organising this type of crimes has become easier than ever.

The Interpol organisation defines two types of cybercrimes :

- Cyber-enabled crime : traditional crimes enabled and easier to make nowadays due to the fast and accessible internet. One can mention financial crimes, cyberwar, cyberterrorism or children pornography.
- Advanced cybercrime : sophisticated attacks against computer hardware and software.

Tools used to combat cybercrime

The first measures to combat cybercrime have been taken by the European countries. The first measures to combat cybercrime have been taken by the European countries. European countries first collaborated with Interpol which aims at making intelligence services exchanges easier and therefore increasing the efficiency of the fight against criminality and cybercriminality.

Europol has also proved its efficiency when it comes to increasing exchanges between national police regarding cybercrime. The European Union has estabished a European Center which struggles against cybercrime within Europol called European Crime Centre (EC3). The EC3 supports the investigations of specialized services of the EU members states concerning several fields, including scams, child pornography and so on. In addition, the EC3 also supports the criminal analysis in the United States, especially by producing analyses on the latest trends in cybercrime and how to combat them.

EUROJUST, which is a EU organ, improves the effectiveness of the authorities of the members states in combating the transborder cybercriminality.

Besides, the ENISA (European Union Agency for Network and Information Security was created in 2004 and is committed to maintain the security of networks and informations. One of its duties is to gather and analyze the data linked to the security-related incidents, besides keeping an eye on the creation of norms for products and services concerning the network and information safety and the promotion of risk management activities.

What is more is that the European programme Safer Internet Plus tackles the illegal content and promotes a safer internet environment.

If it is barely dealt with by the daily news and the most popular media, cybercriminality is a real issue and tackling it happens to be a difficult task with several hurdles. Indeed, networks are numerous, commissions are not always swift, evidences are hard to gather and investigation methods can violate the basic rights, especially the freedom of speech and the right for anonymity.

Cybercrime threats

Cyberterrorism

Cyberterrorism is unquestionably one of the biggest threats deriving from cybercriminality, due to the boundariless internet territory and the hypothesis that cyberterrorism can occur anytime and anywhere.

Cyberwarfare

Driven by civil or military motivations, It is often referred to as « cyberwar » but this term is questioned. Computers can become a weapon in warfare through cyberattacks on network systems, sabotage and espionage. Cyberwarfare can be conducted not only by states, but also by non-state actors, including extremist groups, terrorist organisations or hacktivists, among others. When perpetrated by a state, it is entirely part of the geostrategy and military strategies.

One of the most important cyberwarfare events was held during the 2006 Israeli-Lebanese war. As a matter of fact, the Israel Defense Forces, having great skills in cyberwarfare planning and strong cyberwarfare alliances with Western powers, suspected Hezbollah to operate via Russian hackers.

Cyberextortion (Fraud, phishing scams)

Questions a resolution should address

- Which criminal acts characterize cybercrime?
- Which international treaties and measures have been taken to prevent this issue?
- How could the Interpol collaborate with other international organisations and regional bodies to deal with cybercrime?
- Has the country you are embodying passed laws to tackle cybercrimes? If so, which ones?
- How can your country contribute to fighting against cybercrimes? Which means is it able to supply the Interpol with?
- How to prevent cybercriminals from taking advantage of technology to fulfill their criminal projects?

Sources and Further Readings

http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

https://www.interpol.int/Crime-areas/Cybercrime/The-threats

https://www.interpol.int/Crime-areas/Cybercrime/Activities

https://www.interpol.int/Crime-areas/Cybercrime/Operations

https://www.interpol.int/Crime-areas/Cybercrime/Research

https://www.interpol.int/Crime-areas/Cybercrime/Partners

https://www.interpol.int/Crime-areas/Cybercrime/Online-safety

http://www.nato.int/cps/en/natohq/topics_78170.htm

https://www.fbi.gov/investigate/cyber

http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

http://www.icttf.org/blogs/2/7/european-convention-on-cybercrime