



ERÜNAL SOCIAL SCIENCES HIGH SCHOOL
MODEL UNITED NATIONS CONFERENCE 2025

STUDY GUIDE

INTERPOL

AGENTA ITEM

Illegal trafficking activities in
Deep Web

UNDER SECRETARY GENERAL
Osman Çakır

ERÜNALMUN2025

Table of Contents

1. Letter from the Secretary-General

2. Introduction to The Committee

2.1 Introduction to INTERPOL

2.2 Essential tools that help INTERPOL in their investigations

2.3 Notice System

3. Introduction of Agenda

3.1 Surface Web

3.2 Deep Web

3.3 Dark Web

3.4 Trafficking

3.5 Human Trafficking

3.6 Sex Trafficking

3.7 Labor Trafficking

3.8 Firearms Trafficking

3.9 Organ Trafficking

3.10 Drug Trafficking

3.11 Past Actions of the UN

4. Questions to be Addressed

5. References and Bibliography

1. Letter from the Secretary-General

Honourable participants of ERUNALMUN'25; as the secretariat of this glamorous conference, we are highly welcoming you to this journey. And extending appreciation of ours by thanking all of you one by one for choosing The Legacy of Legend.

Our marvelous academic and organization teams worked intensively, spend months to prepare you the best MUN experience that you could ever see.

Throughout this journey; you will have the chance to debate your ideas by being the part of discussion, improve your negotiation skills, learn new diplomatic terms, enhance your leadership and communication qualifications. And most importantly you will be able to Lead the Light of our future.

We hope you all wonderful committee experience, if you have any issues you are free to contact us

via ozcanramazanrahmi@gmail.com

seloosesn@hotmail.com

Kind regards, Selin Esin & Ramazan Rahmi Özcan
Secretariat of ERUNALMUN'25

2. Introduction to the Committee

Introduction of the Interpol;

The International Criminal Police Organization, known as INTERPOL, facilitates worldwide police cooperation and crime control. Headquartered in Lyon, France, it is the world's largest international police organization, with seven regional bureaus worldwide and a National Central Bureau in all 196 member states. Interpol was conceived during the first International Criminal Police Congress in 1914, which brought officials from 24 countries to discuss cooperation in law enforcement. It was founded on September 7, 1923, at the close of the five-day 1923 Congress session in Vienna as the International Criminal Police Commission (ICPC); it adopted many of its current duties throughout the 1930s. After coming under Nazi control in 1938, the agency had its headquarters in the same building as the Gestapo. It was effectively moribund until the end of World War II. In 1956, the ICPC adopted a new constitution, and the name Interpol, derived from its telegraphic address used since 1946.

Interpol provides investigative support, expertise, and training to law enforcement worldwide, focusing on three major areas of transnational crime: terrorism, cybercrime, and organized crime. Its broad mandate covers virtually every kind of crime, including crimes against humanity, child pornography, drug trafficking and production, political corruption, intellectual property infringement, as well as white-collar crime. The agency also facilitates cooperation among national law enforcement institutions through criminal databases and communications networks. Contrary to popular belief, Interpol is not a law enforcement agency.

Interpol has an annual budget of €142 million, most of which comes from annual contributions by member police forces in 181 countries. It is governed by a General Assembly composed of all member countries, which elects the executive committee and the President (currently Ahmed Naser Al-Raisi of the United Arab Emirates) to supervise and implement Interpol's policies and administration. Day-to-day operations are carried out by the General Secretariat, comprising around 1,000 personnel from over 100 countries, including both police and civilians. The Secretariat is led by the Secretary-General, currently Valdecy Urquiza of Brazil, appointed by the 92th General Assembly session.

Pursuant to its charter, Interpol seeks to remain politically neutral in fulfilling its mandate, and is thus barred from interventions or activities that are political, military, religious, or racial in nature and from involving itself in disputes over such matters. The agency operates in four languages: Arabic, English, French and Spanish.

Essential Tools that help Interpol in their investigations;

Stolen and Lost Travel Documents (SLTD): SLTD database contains information on travel and identity documents that have been reported as stolen, lost, revoked, invalid or stolen blank. Law enforcement officers around the world can check the validity of a travel or identity document in seconds using the SLTD database.

Automatic Fingerprint Identification System (AFIS): Authorized users in member countries can cross-check records from their national fingerprint databases against AFIS, where they think there may be an international aspect to the crime.

Notice System: INTERPOL also has the function of informing other member countries, the United Nations and the public. This action is done through **notices**. Notices are published by the General Secretariat at the request of the National Central Bureau to whom it may concern.

I) Red Notice: To seek the location and arrest of persons wanted for prosecution or to serve a sentence.

II) Yellow Notice: To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.

III) Blue Notice: To collect additional information about a person's identity, location, or activities in relation to a criminal investigation.

IV) Black Notice: To seek information on unidentified bodies.

V) Green Notice: To provide warning about a person's criminal activities, where the person is considered to be a possible threat to public safety.

VI) Orange Notice: To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.

VII) Purple Notice: To seek or provide information on modus operandi, objects, devices, and concealment methods used by criminals.

VIII) United Nations Security Council Special Notice: Issued for entities and individuals who are the targets of UN Security Council Sanctions Committees.

NOTICES PUBLISHED PER YEAR							
							
2017							
12,042	2,508	4,422	130	777	3	165	19
2018							
13,516	2,397	4,139	134	827	52	97	28
2019							
13,410	3,193	3,375	256	761	33	92	15
2020							
11,094	2,554	3,966	391	509	39	130	9
2021							
10,776	2,622	3,604	118	1,072	45	107	13

Introduction of Agenda

Surface Web;

The Surface Web, also known as the Visible Web, is the portion of the Worldwide Web that is readily available and accessible by standard web search engines.

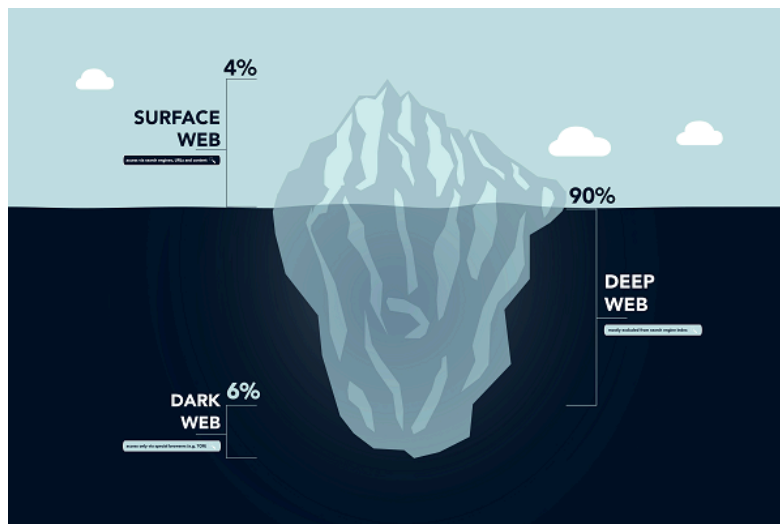
Deep Web;

The Deep Web or The Invisible Web are the parts of the Worldwide Web that are not accessible by standard web search engines. Deep Websites can be accessible through a direct URL or IP address but may require a password or other security information to access the actual content. This can include webmail, private databases, web forums that require registration, and restricted-access social media profiles. Deep Web also includes the Dark Web.

Dark Web;

The Dark Web is the part of the Worldwide Web that requires specific software, authorization, or configurations to access. Private computer networks can communicate or conduct business anonymously through the dark web without revealing identifying information, such as a user's location. It operates on networks like TOR (The Onion Router), designed to conceal users' identities, information, and locations. Unlike the other parts, the Dark Web forms a small part of the deep web but requires custom software and configurations.

And why do criminals commonly use the dark web? The main reason that criminals often use the dark web is that it offers an increased layer of protection. Given this private nature, the dark web has become an outlet for individuals with malicious intentions who want to reach a larger group of potential victims. Since the dark web has become a common standpoint for criminals, it can contain a wide range of illegal activities such as murder for hire, blackmail, types of trafficking, terrorism, and child pornography, trafficking being the most common one.



Scheme of the Layers of Web

The Onion Router (TOR);

Free and open-source software that enables anonymous communication. TOR is the most common tool used to access the dark web.

Cryptocurrency;

Cryptocurrency is a digital currency designed to work through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it, which makes it more discreet in money transactions.

Trafficking;

Trafficking or smuggling is the illegal transportation of objects, substances, information, or people, in violation of applicable laws or regulations. With the development of technology, it has become much easier for ill-intended people to find potential targets/recruits and new strategies for trafficking purposes. The dark net is most commonly used for the purpose of trafficking.

Human Trafficking;

Human Trafficking is the recruitment, transportation, transfer, harboring, or receipt of people through force, fraud, or deception, with the aim of exploiting them for profit. Men, women, and children of all ages and from all backgrounds can become victims of this crime, which occurs in every region of the world.

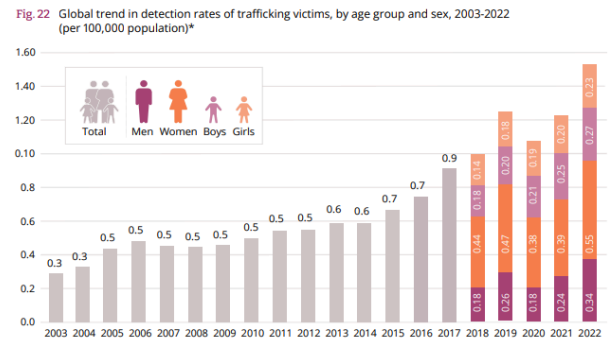


Figure SEQ Figure 1* ARABIC 1

As can be seen in Figure 1, as technology developed over the years, human trafficking rates have increased in alignment. According to the statistics of Polaris Analysis of 2020 and 2021 Trafficking data in the U.S., 72% of the human trafficking victims in 2020 and 63% in 2021 have been recruited online in certain platforms.

Where does the Dark Web play a role in this?

Considering the fact that the dark web is a haven for illicit activities, traffickers have naturally found their way there.

The Dark Web can be a huge database for traffickers when it comes to picking and recruiting victims. The privacy of the dark web makes it easier to exchange information about victims, and share victim profiles and tips and techniques on how to lure them; practically creating a network of exploitation.

Discreet facilitation of money transactions is also one of the outstanding Dark Web functions when it comes to such activities. The use of **cryptocurrencies** for this purpose makes it very discreet and hardly trackable which enables traffickers to engage in illegal deals without raising any suspicion.

When it comes to hosting **Child Sexual Abuse Material (CSAM)** the dark web is the first place that comes to mind. The dark web is the main tool in producing and distributing CSAM.

Child Sexual Abuse Material (CSAM); Any sort of sexually explicit visual content involving a minor is CSAM, also known as Child Pornography. This can include photographs, videos, and any computer/Artificial intelligence generated images.

CSAM is often produced by online solicitation, coercion, covert photography (unconsensually taking explicit pictures of someone unaware of it), or rape. However, such pictures of minors are often produced by themselves without the presence of an adult hence some coercion/manipulation methods online sex offenders use to acquire these pictures without force.

What are the traffickers' ways to lure victims online?

Traffickers often use deceptive methods to lure victims. They may pose as potential romantic partners, modeling scouts, or job agencies offering promises of jobs or education. They may groom victims online and detect their vulnerabilities to exploit them. Traffickers can also use social media information to identify, locate, or collect information about their victims. Such methods as blackmail, threatening, use of status or a position, etc. can be used to push the victims into nonconsensual activities after their information is collected by a trafficker.

Trafficking online, as broad as it is, can be divided into five categories being Labor Trafficking, Sex Trafficking, Firearms Trafficking, Organ Trafficking, and Drug Trafficking.

Labor Trafficking;

Labor trafficking is a form of **human trafficking** in which individuals perform labor or services through the use of force, fraud, or coercion. Traffickers use hidden forums and marketplaces to advertise fraudulent job opportunities, often in high-demand fields, to lure victims. These ads may promise high wages, desirable working conditions, and opportunities for

immigration. Once victims are recruited, traffickers use the dark web to coordinate transportation, housing, and payment schemes, often involving cryptocurrencies to obscure financial trails.

The consequences of labor trafficking on the dark web are severe. Victims are subjected to forced labor, often in dangerous and exploitative conditions. They may be physically and emotionally abused, denied basic necessities like food and healthcare, and deprived of their freedom and human rights. Additionally, labor trafficking on the dark web undermines legitimate businesses, distorts labor markets, and fuels other criminal activities.

Sex Trafficking;

Sex trafficking is a type of **human trafficking** for sexual exploitation. It can also be a sub-category of labor trafficking when it engages in sexual labor. Perpetrators of the crime are referred to as sex traffickers— people who manipulate victims to engage in various forms of commercial sex with paying customers. Target victims of this crime are usually women and children.

Sex trafficking in the dark web can have several variations, some of these being the production and distribution of CSAM, abduction, and transportation of victims by luring them online into face-to-face meetings, and online escort services.

Another variation to online sex trafficking is **cybersex trafficking** which is live-streamed rape/sexual abuse which is the manipulation and forcing of victims into performing sexual acts in front of a camera for the financial gain of the trafficker or the viewers.



Firearms Trafficking

Firearms trafficking, also known as gun trafficking, is the illegal trade of firearms and ammunition. It's a global problem with significant consequences, fueling violence and instability in many regions. In the dark web, firearms products are usually listed as; firearms, ammunition, parts and components, and explosives. There are, at present, two types of marketplaces found on the dark web where firearms and related products are offered and sold: cryptomarkets and vendor shops.

Cryptomarkets are online platforms that facilitate buying and selling goods or services using cryptocurrencies. They operate similarly to traditional e-commerce marketplaces, with features like **escrow** (where the buyer's payment is held by the platform until the buyer confirms receipt of the goods) to hold payments until buyers confirm receipt and dispute resolution mechanisms to address potential issues. To help buyers make informed choices, these platforms often include customer ratings and reviews for each seller. While offering some level of anonymity and potentially facilitating legitimate transactions, many crypto markets are associated with illegal activities.

Vendor shops are online stores run by individual sellers, offering a more direct sales channel compared to crypto markets. By bypassing the marketplace, vendors avoid paying commissions and the risk of losing

funds in "exit scams" where the platform disappears with customer funds. These shops often specialize in specific products and rely on their established reputation from previous cryptomarket sales to build trust with customers. While some vendors continue to operate on cryptomarkets, they utilize vendor shops for direct sales. To minimize detection, firearms are often disassembled and shipped in separate packages.

Organ Trafficking

Organ trafficking is the act of taking one's organs for the purpose of illegal sales and transplantation without the individual's consent.

Similar to other forms of trafficking, victims are picked and recruited with the help of the dark web, and traffickers often communicate their plans through the dark web. Cryptomarket also comes in handy the same way for organ trafficking hence the anonymity of it.

Once victims are recruited, they are coerced into having their organs removed or they are unaware of it. The organs are usually removed in unsanitary and unsafe conditions, often without proper medical care.

Global Financial Integrity (GFI) estimates that 10 percent of all organ transplants including lungs, heart, and liver, are done via trafficked organs.¹ However, the most prominent organs that are traded illicitly are kidneys, with the World Health Organization (WHO) estimating that 10,000 kidneys are traded on the black market worldwide annually, or more than one every hour.

Drug Trafficking

Drug trafficking, also known as drug smuggling or narcotrafficking, is the illegal cultivation, manufacture, distribution, and sale of substances that are subject to drug prohibition laws. It is a global black market driven by high profits and demand.

Customers intending to buy drugs over the darknet typically access it through the onion router (TOR) to conceal their identities. Specialized darknet explorers (such as GRAMS, before it was taken down in December 2017) enable them to access their desired market platforms. The goods bought on the various darknet marketplaces are then typically paid for in cryptocurrencies.

Past Actions of the UN

UNODC

The 2020 UNODC Darknet Threat Assessment Report: The 2020 UNODC Darknet Threat Assessment Report delves into the evolving landscape of criminal activity facilitated by the darknet, providing a comprehensive overview of the challenges law enforcement and policymakers worldwide faces. The report highlights the increasing diversity of illicit goods and services available on the darknet, with a particular focus on the proliferation of synthetic drugs, opioids, and their precursors. It also emphasizes the growing role of the darknet in trafficking weapons, counterfeit goods, and stolen data.

Furthermore, the report underscores the escalating sophistication of cybercrime techniques employed by darknet actors. The report highlights the financial incentives driving these activities, with cybercriminals often exploiting vulnerabilities in critical infrastructure and personal devices to extort large sums of money.

The report also acknowledges the challenges faced by law enforcement in combating darknet-related crime. The report calls for increased international cooperation, technological innovation, and capacity-building efforts to effectively address the evolving threats posed by the darknet.

Operation SpecTor: Operation SpecTor was a major international law enforcement operation targeting the darknet trafficking of fentanyl and other opioids. Led by the Justice Department's Joint Criminal Opioid Darknet Enforcement (JCODE) team and UNODC played a key role in supporting of this operation, it involved nine countries across three continents, including the United States, Europe, and South America. The operation resulted in a significant number of arrests, seizures of illicit drugs, and the disruption of darknet marketplaces like Monopoly Market. It showcased the increasing collaboration between law enforcement agencies worldwide in combating the global threat of darknet-facilitated drug trafficking, demonstrating the potential for international cooperation to disrupt criminal networks operating in this space.

Global Programme for Cybercrime Prevention and Criminal Justice: The UNODC Global Programme on Cybercrime is a multi-faceted initiative designed to assist countries in effectively combating cybercrime. It focuses on building the capacity of law enforcement and judicial officials through training programs and resource sharing, supporting the development of robust legal frameworks that align with international standards, fostering international cooperation among law enforcement agencies, and raising public awareness about cybercrime risks and promoting responsible online behavior. By addressing these key areas, the program aims to strengthen the global response to cybercrime and create a safer online environment for all.

INTERPOL

Operation Turquesa: Operation Turquesa is a collaborative initiative between INTERPOL and the United Nations Office on Drugs and Crime (UNODC) aimed at combating migrant smuggling and human trafficking in the Americas. This multi-faceted operation involves a comprehensive

approach to disrupt criminal networks exploiting vulnerable individuals for profit. Key components of Operation Turquesa include in-depth criminal analysis to identify key players and vulnerabilities, capacity building for law enforcement and border officials to enhance their skills in identifying, investigating, and prosecuting migrant smuggling and human trafficking cases, and coordinated law enforcement actions across countries, including targeted arrests, seizures of assets, and rescue operations to dismantle criminal networks and protect victims.

Project I-Core: Project I-Core is a 10-year INTERPOL initiative that aims to enhance global policing capabilities by modernizing its infrastructure and strengthening its operational capacities. This ambitious project focuses on seven key areas: improving the quality, accessibility, and sharing of criminal data; strengthening forensic capabilities to collect, analyze, and share evidence more effectively; countering cybercrime by enhancing law enforcement's capacity to investigate and disrupt online criminal activities; combating terrorism by improving intelligence sharing, operational coordination, and investigative techniques; disrupting organized crime networks by enhancing cross-border cooperation, intelligence sharing, and asset recovery efforts; addressing environmental crime by strengthening law enforcement's capacity to investigate and combat illegal wildlife trafficking, illegal logging, and other environmental offenses; and countering corruption by enhancing international cooperation and investigative techniques to combat bribery, money laundering, and other forms of corruption.

Through these key areas, Project I-Core seeks to equip law enforcement agencies worldwide with the tools, resources, and expertise needed to effectively address the evolving challenges of transnational crime in the 21st century. It aims to foster closer collaboration among law enforcement agencies, improve information sharing, and enhance operational capabilities to better prevent, investigate, and respond to criminal threats.

Operation Synergia II: Operation Synergia II was a major global law enforcement operation led by INTERPOL that targeted cybercriminals involved in phishing, ransomware, and information-stealing activities. This collaborative effort involved law enforcement agencies from an unprecedented 95 countries, demonstrating a significant increase in international cooperation to combat cybercrime.

The operation resulted in a substantial impact, with over 22,000 malicious servers taken down and 41 individuals arrested. This disruption of criminal infrastructure and apprehension of key actors significantly disrupted the activities of cybercriminal networks operating globally.

Operation Synergia II highlights the growing threat of cybercrime and the critical need for international collaboration to effectively counter these threats. By pooling resources, sharing intelligence, and coordinating law enforcement actions, countries can more effectively disrupt cybercriminal activities, protect critical infrastructure, and safeguard individuals from online threats.

Project Libertad: Interpol's Project Libertad is a global operation targeting online child sexual exploitation and abuse, specifically the distribution and consumption of Child Sexual Abuse Material (CSAM) on the darknet. This coordinated effort involves law enforcement agencies worldwide, utilizing advanced data analysis to identify and track online predators. Undercover operations are conducted to apprehend individuals involved in the distribution of CSAM, and international cooperation is crucial in sharing information and coordinating efforts across borders. The ultimate goals of Project Libertad are to disrupt online networks involved in the production and distribution of CSAM, identify and apprehend offenders, and protect children from sexual abuse.

Questions to be Addressed

- 1. What can be done to protect vulnerable individuals from traffickers?*
- 2. What can be done to prevent trafficking on the dark web?*
- 3. How can the member states prevent the Dark Web from spreading for malicious purposes?*
- 4. Which other UN bodies or NGO's can be cooperated with, in regards to tackling trafficking over the darknet?*
- 5. What measures can be taken in order to prevent traffickers from grouping and forming trafficking databases?*
- 6. How to decrease the increasing demand towards drugs and illicit firearms?*
- 7. What can be done to reduce the psychological burden of human trafficking survivors? How to help them?*

8. *How can the INTERPOL ensure the accuracy of worldwide data that is collected upon trafficking over the dark web ?*

References and Bibliography

https://en.wikipedia.org/wiki/Surface_web

https://en.wikipedia.org/wiki/Deep_web

https://en.wikipedia.org/wiki/Dark_web

<https://www.findlaw.com/criminal/criminal-charges/dark-web-crimes.html>

<https://www.statista.com/topics/11491/dark-web/#topFacts>

<https://en.wikipedia.org/wiki/Smuggling>

<https://news.un.org/en/story/2021/10/1104392>

<https://traffickinginstitute.org/wp-content/uploads/2022/01/2020-Federal-Human-Trafficking-Report-Low-Res.pdf>

<https://www.unodc.org/unodc/en/human-trafficking/human-trafficking.html>

<https://www.unodc.org/unodc/en/human-trafficking/crime.html>

<https://eightdaysofhope.com/app/uploads/2022/11/Human-Trafficking-Statistics-and-Online-Safety.pdf>

<https://polarisproject.org/wp-content/uploads/2020/07/Polaris-Analysis-of-2021-Data-from-the-National-Human-Trafficking-Hotline.pdf>

<https://www.ic3.gov/PSA/2020/PSA200316>

<https://enactafrica.org/enact-observer/youth-lured-by-the-false-promise-of-well-paid-jobs>

https://en.wikipedia.org/wiki/Child_pornography

<https://humantraffickinghotline.org/en/human-trafficking/labor-trafficking>

<https://www.unodc.org/lpo-brazil/en/trafico-de-pessoas/ungift.html>

https://en.wikipedia.org/wiki/Organ_theft

<https://www.acamstoday.org/organ-trafficking-the-unseen-form-of-human-trafficking/>

<https://front.un-arm.org/wp-content/uploads/2018/10/occasional-paper-32.pdf>

https://www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf

<https://www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results>

<https://www.unodc.org/westandcentralafrica/en/Cyber-Crime.html>

<https://www.interpol.int/Crimes/Human-trafficking-and-migrant-smuggling/Project-Turquesa>

<https://www.interpol.int/How-we-work/I-CORE-our-vision-for-change>

<https://www.interpol.int/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats>