2025

EKIN SNY MUN BACKGROUND GUIDE

Committee: INTERPOL

Topic: Disrupting Criminal Activity on the Dark Web

ekinjmun@gmail.com

www.ekinjmun.org

Table of contents

WELCOME SPEECH/LETTER FROM THE CHAIRBOARD

Dear Delegates,

We welcome you to the annual Ekin Junior Model United Nations Conference! We are honored to serve as your chairboard and look forward to fruitful discussions and productive sessions!

I am Derin Açıkel and I will be serving as your president chair throughout the conference. I am currently a junior in Ekin College High School and this is going to be my 20th experience so far. Because of my keen interest in law enforcement and preventing cybercrime, I specifically picked this topic and I deeply hope that you will enjoy the agenda and come up with brilliant ideas. This guide will help with your research and help you understand the topic, but I would like to inform you that it is your duty to dig deeper and root your research. As the chairboard, we have worked hard to ensure that this committee provides you with engaging discussions and lots of new information.

I am excited to witness your skills and creativity while assisting you throughout the debates. If you have any questions, please feel free to reach out to us before or during the conference.

Best regards,
Derin Açıkel
Chair

The International Criminal Police Organization

The International Criminal Police Organization (INTERPOL) is an intergovernmental organization that coordinates policing efforts between police organizations. The idea of addressing crimes at an international level was introduced at the first Criminal Police Congress, held in Monaco in April 1914 and attended by representatives from 20 countries.

INTERPOL was founded in 1923 following World War I as the International Criminal Police Commission (ICPC). It aimed to provide mutual assistance between police forces in different countries. The ICPC became the International Criminal Police Organization (ICPO-INTERPOL) in 1956. The organization now assists police forces in 195 countries around the world in deterring crime by facilitating data sharing on crimes and criminals and offering technical support.

While the General Secretariat coordinates INTERPOL's daily operations, it is led by the Secretary-General and staffed by police and civilians. The organization's headquarters are in Lyon, France, and its global innovation center is in Singapore, with other offices in various locations. A National Central Bureau (NCB) exists in every country to oversee INTERPOL matters. Each country's NCB is housed in the corresponding governmental ministry in charge of policing and managed by national police officials. INTERPOL's governing body is the General Assembly, which gathers all nations once annually to make decisions.

Definitions

Surface Web: A part of the internet that is publicly accessible.
Deep Web: A part of the internet that is not publicly accessible and which mostly consists of private accounts, sites, and content that requires payment/subscription.
Dark Web: A hidden part of the internet that is only accessible through specialized software.
Tor: A special network that encrypts user data and grants anonymous browsing.
Encryption: A security measure that protects your data from unauthorized access.
IP Address: This acronym stands for "Internet Protocol Address." This is a unique identifying label or number for each device or network connected to the internet.
VPN: This acronym stands for "Virtual Private Network." It is a service that encrypts the internet connection and hides a user's IP Address to protect their identity and secure their privacy.

Shock Content: Disturbing and explicit images or videos that trigger strong emotional reactions from viewers.
U.S. NRL: The United States Naval Research Laboratory.
Cryptocurrency: Digital and secured currency mostly used for transactions on the web such as Bitcoin, Monero, and Zcash.
Ransomware: A type of software that steals a victim's data and demands payment in order to give it back.
PGP: This acronym stands for "Pretty Good Privacy." It is an encryption program that ensures that only the authorized user can access the data.
Blockchain: A digital notebook that keeps records of transactions across multiple computers by putting data in segments called blocks.
MFA: This acronym stands for Multi-Factor Authentication. It is an electronic authentication method that requires a user to pass two or more authentication steps before gaining access to an application or website.
KYC: This acronym stands for Know Your Customer. Financial institutions use these guidelines to verify their customers' identities and assess the risk of potential fraud or money laundering.
Biometric authentication: This is a security process that helps verify a user's identity through unique physical traits such as their face or fingerprints.
AI: Artificial intelligence. It refers to the enhanced ability of computers and robots to simulate human intelligence to perform tasks.

Introduction to the Topic

The Internet is divided into three layers: the Surface Web, the Deep Web, and the Dark Web. The Surface web is the most used layer of the internet and consists of publicly accessible, safe, and legal websites. These websites can be reached through commonly used search engines such as Google and Yandex. Despite being used worldwide by billions of people every day, it only covers approximately 5% of the internet.

After the Surface Web, there is the Deep Web which is mostly misunderstood. The Deep Web, for the most part, corresponds to password-encrypted sites and private databases. It is not completely illegal. Private social media accounts, digital banking platforms, electronic mail (e-mail), and messaging apps are all considered a part of the Deep Web. The Deep Web keeps users' data secure and helps with anonymity. It is important to acknowledge that the Deep Web and the Dark Web are not the same but two different layers of the internet with different purposes.

What is the Dark Web?

The Dark Web is a part of the Deep Web that is hidden from public view and popularly used for illegal activities. It is extremely dangerous to access even with a very secure browser; a single mistake could be very costly. The Dark Web is only accessible through special configurations and software, including browsers specifically used to access it.

There is a diverse range of content, both legal and illegal on the Dark Web. Indeed, while it can provide a secure and anonymous platform for journalists and activists, it can also facilitate the conduct of illegal activities such as drug and weapon sales, human trafficking, fraud, and identity theft. It is very common to come across scams, viruses, and different types of shock content on the Dark Web as well as extremely disturbing sites that go against human rights. The sites on the Dark Web use complex encryptions which make them almost completely inaccessible through ordinary browsers.

Evolution of the Web

The history of the web dates back to the 1990s, when the United States Naval Research Laboratory (U.S. NRL) developed Tor for governmental communications and launched it in 2002 as a private network for internet browsing. Since Tor grants its users anonymity on the web and online safety, the developers had unknowingly paved the way for the development of the Dark Web. After 2010, the Dark Web became a hub for illegal activities following the rise of Bitcoin transactions.

The first darknet marketplace that was accessed through Tor and which used Bitcoin as a currency was a site called Silk Road. It was created by Ross Ulbricht, who was also known as “Dread Pirate Roberts,” in 2011. The infamous marketplace provided users with a wide range of both legal and illegal products and services. These included drugs, falsified documents, hacking services, weapons, counterfeit money, and stolen tech items. On May 29, 2015, Ulbricht was sentenced to life in prison without the possibility of parole but he was granted a presidential pardon from U.S. President Donald Trump in January 2025.

Anonymity

In order to access the Dark Web, one must go through multiple domains and different browsers; the most commonly used one is “Tor Browser” which uses “onion routing”. The term “onion routing” comes from data passing through different layers, like the layers of an onion. This corresponds to a data encryption and transmission method that is used to protect anonymity and privacy on the web. In other words, onion routing allows an individual to hide their personal data and makes it harder for them to be tracked online. To elaborate, when taking an action on the web, this action is encrypted multiple times before being executed. It gets sent through randomly generated and selected destinations before being transmitted without revealing a user’s identity.

The suffix “.onion” is often used in association with the Tor network. Peer-to-peer networks also distribute data through multiple layers and make it harder to trace the origin of this data. Usage of Virtual Private Networks (VPNs) to increase your anonymity is likewise common on the Dark Web; even though it is not obligatory, it significantly enhances one’s privacy and masks the user’s Internet Protocol (IP) address. Additionally, people use “pseudonyms,” which are basically nicknames or fake identities to hide their own. These methods do protect one’s anonymity, but no system is entirely safe; even though it is a remote possibility, one’s identity could possibly be uncovered despite their best efforts.

Transactions

Transactions on the Dark Web operate through a complex system designed to ensure anonymity and security by using cryptocurrencies instead of traditional online transactions—the most popular one being Bitcoin. In addition to Bitcoin, and because of law enforcement agencies’ improved abilities to track down Bitcoin, Monero and Zcash have gained popularity among users.

Payments first go through escrow services, where the funds are held safely until the buyer confirms the transaction. Vendors often use “Pretty Good Privacy” (PGP), similar to how buyers use Tor to preserve their data and guarantee their anonymity. However, even with multiple measures in place to secure anonymity, departments that analyze blockchains such as Chainalysis can still track suspicious activity to help law enforcement agencies uncover marketplaces on the Dark Web.

Types of Criminal Activities

The Dark Web marketplace is enormous, with thousands of different illegal goods as well as services such as hiring hitmen or hackers. In other words, the Dark Web serves as a center for a number of criminal operations. These include:

Drug Trafficking: One of the most common activities on the Dark Web is the sale of illegal narcotics. Vendors sell anything from hard drugs to prescription medications and they frequently send them covertly to customers all around the world.

Weapons Trade: Bypassing conventional laws and background checks, it is possible to buy firearms, explosives, and other weapons anonymously.

Human Trafficking: Forced labor and sex trafficking are among the activities that are made possible by certain Dark Web communities.

Fraud and Financial Crimes: The Dark Web is full of fake passports, counterfeit money, stolen credit card information, and other illegal services.

The Impact of the Dark Web on a Global Level

The Dark Web significantly impacts global stability and cybersecurity. Important effects include an increase in cybercrime, such as ransomware, identity theft, and corporate espionage, all made possible by the anonymity provided by the Dark Web.

The main impacts and challenges presented by the Dark Web are as follows:

- **Threats to National Security:** Criminal and terrorist groups use the Dark Web to exchange information, finance their activities, and obtain illegal goods.
- **Challenges for Law Enforcement:** Because of encryption and decentralized networks, governments and international organizations find it difficult to monitor and disrupt illicit activities.
- **Financial Implications:** Illicit transactions, which upend economies, make money laundering and tax evasion possible globally.
- **Ethical and Moral Concerns:** The Dark Web's unregulated state raises ethical questions about digital rights, privacy, and surveillance.

Suggestions or Recommendations for Monitoring the Web

Key among the recommendations to disrupt criminal activity on the Dark Web is improving monitoring activities and enhancing cybersecurity. This includes:

- **Implementing Additional Authentication Methods:** Requiring multi-factor authentication (MFA) for Bitcoin transactions can make illegal trade more difficult. Know Your Customer (KYC) procedures for transactions should also be strengthened to lessen anonymity. Biometric authentication should additionally be required for critical transactions.

- **Further Improving Blockchain Monitoring Systems:** This can be done through increasing the tracking of suspicious activity by using blockchain analytics powered by artificial intelligence (AI). It also includes strengthening cooperation to identify illegal transactions with Bitcoin exchanges. Systems like Chainalysis identify financial trends on the Dark Web.

- **Collaboration Across Nations:** This can take many forms, such as establishing more powerful multinational task teams to fight cybercrime, promoting agreements across law enforcement organizations for information sharing, and strengthening international legislation to prevent cryptocurrency abuse on the Dark Web.

Questions to Consider

1. What legislation does your country have in place to combat crimes on the web and guarantee its cybersecurity?
2. How can law enforcement agencies strike a balance between privacy rights and Dark Web surveillance?
3. What ethical challenges arise from governments monitoring cryptocurrency transactions?
4. How effective are blockchain analysis tools in preventing illegal transactions?
5. What role do major tech companies play in combating Dark Web activities?
6. How can international cooperation be improved to fight illicit Dark Web markets?

RESEARCH AID/REFERENCES

1 The International Criminal Police Organization, “How Our History Started,” https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started.

2 Tunale University School of Professional Advancement, “Everything You Should Know About the Dark Web,” Tulane University, https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web.

3 Congressional Research Service, “The Dark Web: An Overview,” Congressional Research Service Report In Focus, 2 December 2024, https://crsreports.congress.gov/product/pdf/IF/IF12172/3.

4 Department of Justice - Office of the Inspector General - Audit Division, “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities,” December 2020, https://oig.justice.gov/sites/default/files/reports/21-014.pdf.

REFERENCES

- "Child Mortality: An Overview," Science Direct, https://www.sciencedirect.com/topics/social-sciences/child-mortality.

- Bernadette O'Hare, Innocent Makuta, Levison Chiwaula, and Naor Bar-Zeev, "Income and Child Mortality in Developing Countries: A Systematic Review and Meta-Analysis," Journal of the Royal Society of Medicine 106, no. 10 (2013): 408—14, https://pmc.ncbi.nlm.nih.gov/articles/PMC3791093/.

- Central Intelligence Agency, "Country Comparisons: Infant Mortality Rate," The World Factbook, 2024, https://www.cia.gov/the-world-factbook/field/infant-mortality-rate/country-comparison/.

- Child Health Task Force, "Child Survival Action," 2024, https://www.childhealthtaskforce.org/hubs/child-survival-action.

- Lucia Mullen, "How Has the WHO Responded to the COVID-19 Pandemic?," IPI Global Observatory, 30 April 2020, https://theglobalobservatory.org/2020/04/how-has-who-responded-to-covid-19-pandemic/.

- Peter Beech, "World Health Organization: What Does It Do and How Does It Work?," World Economic Forum, 17 April 2020, https://www.weforum.org/stories/2020/04/world-health-organization-what-it-does-how-it-works/.

- Pien Huang, "Explainer: What Does the World Health Organization Do?," NPR, 28 April 2020, https://www.npr.org/sections/goatsandsoda/2020/04/28/847453237/what-is-who-and-what-does-it-do.

- **UNICEF, “Child Mortality,” March 2024,** https://data.unicef.org/topic/child-survival/under-five mortality/#:~:text=The%20under%2Dfive%20mortality%20rate,dying%20every%20day%20in%202022.

- **UNICEF, “Child Survival and the SDGs,” March 2024,** https://data.unicef.org/topic/child-survival/child-survival-sdgs/.

- **UNICEF, “Levels and Trends in Child Mortality: Report 2023,” United Nations Inter-Agency Group for Child Mortality Estimation (UN IGME), 2024,** https://data.unicef.org/resources/levels-and-trends-in-child-mortality-2024/.

- **UNICEF, “Levels and Trends in Child Mortality: Report 2022,” Save the Children Child Rights Resource Centre, 2023,** https://resourcecentre.savethechildren.net/document/levels-and-trends-in-child-mortality-report-2022/.