FISMUN'24

UNITED NATIONS OFFICE ON DRUGS AND CRIME

Deliberating upon Countering the Use of Information and Communications Technologies for Criminal Purposes

Co-Chairs: Kshitij Saha, Nandita Dey
Moder: Anaga Anil

Contents

Letter from the Executive Board

Dear Delegates,

It gives us great honor and immense pleasure to welcome you all to the United Nations Office on Drugs and Crime at FISMUN, 2024. As representatives of member nations of the Committee, you are tasked with debating, deliberating, and reaching a consensus on the agenda at hand. This background guide has been designed to help you get started on your research. However, the Background Guide should not be your only source of research. Building upon the outlook presented by the Background Guide, you are expected to carry out your research through authentic sources and make sure to engage in comprehensive and pragmatic debate throughout the sessions. The Background Guide has been drafted thoroughly to ensure a holistic overview of the Agenda which can help you better understand the crux of the issues at hand and how to direct the Committee toward the desirable direction in order to achieve consensus and address the issues being discussed in the Committee.

The Executive Board will not interfere in the flow of debate substantively unless absolutely required. Therefore, the onus to ensure that the Committee does not stagnate lies on the delegates. We strongly believe that with good research, the Delegates will be able to steer the committee in the right direction.

That being said, we sincerely hope that all delegates maintain the highest standards of decorum during the conference days. Remember, you must emulate the behavior of a diplomat representing your portfolio to the best of your ability. Please do not hesitate to get in touch with the Executive Board at any time before or during the Conference if you have any queries about the agendas or the rules of procedure. Further, we have added one addendum to this letter that talks about the nature of evidence entailed in this simulation.

We request the delegates not to view this conference as a zero-sum game. Model UN conferences are collaborative rather than competitive and we would like to keep this spirit alive during our Committee. All of us, collectively, are entrusted with a task greater than winning a prize, that is, to do justice to the responsibility of finding solutions to one of the more critical and challenging problems the world is facing today and to educate ourselves about them, thereby ensuring that we go on to become a generation of sensitized leaders, equipped with the skills and desire to make our world a better place. With the sincere hope that you take home substantial insights about the issue at hand – we know, we will, looking forward to seeing you soon!

Our best,

Kshitij Saha
Co- Chairperson
kshitijgsaha@gmail.com

Nandita Dey
Co- Chairperson
nanditadey0703@gmail.com

Anaga Anil
Moderator
anaga.anil20082008@gmail.com

Addendum: Nature and Proof of Evidence

Documents from the following sources will be considered as credible proof for any allegations made in committee or statements that require verification:

1. Reuter: Appropriate Documents and articles from the Reuters News agency will be used to corroborate or refute controversial statements made in committee.
2. UN Documents: Documents by all UN agencies will be considered sufficient proof. Reports from all UN bodies including treaty-based bodies will also be accepted.
3. National Government Reports: Government Reports of a given country used to corroborate an allegation on the same aforementioned country will be accepted as proof. The documents stated above will hold a binding nature of the establishment.
4. **Other sources** like Wikipedia, Amnesty International, or newspapers like the Guardian, and so on and so forth will not be accepted as credible proof; but may be used for a better understanding of any issue and even be brought up in debate if the information given in such sources is in line with the beliefs of a government or a delegate.

Please note that while background guides are supposed to provide the delegates with an overview of the agenda and further point them towards the right direction for further research, they are not considered valid sources of information and hence cannot be cited as proof of a fact at any point during the committee. Only the above-mentioned sources can be accepted as credible sources of evidence if asked for by the Executive Board.

Overview of the Committee

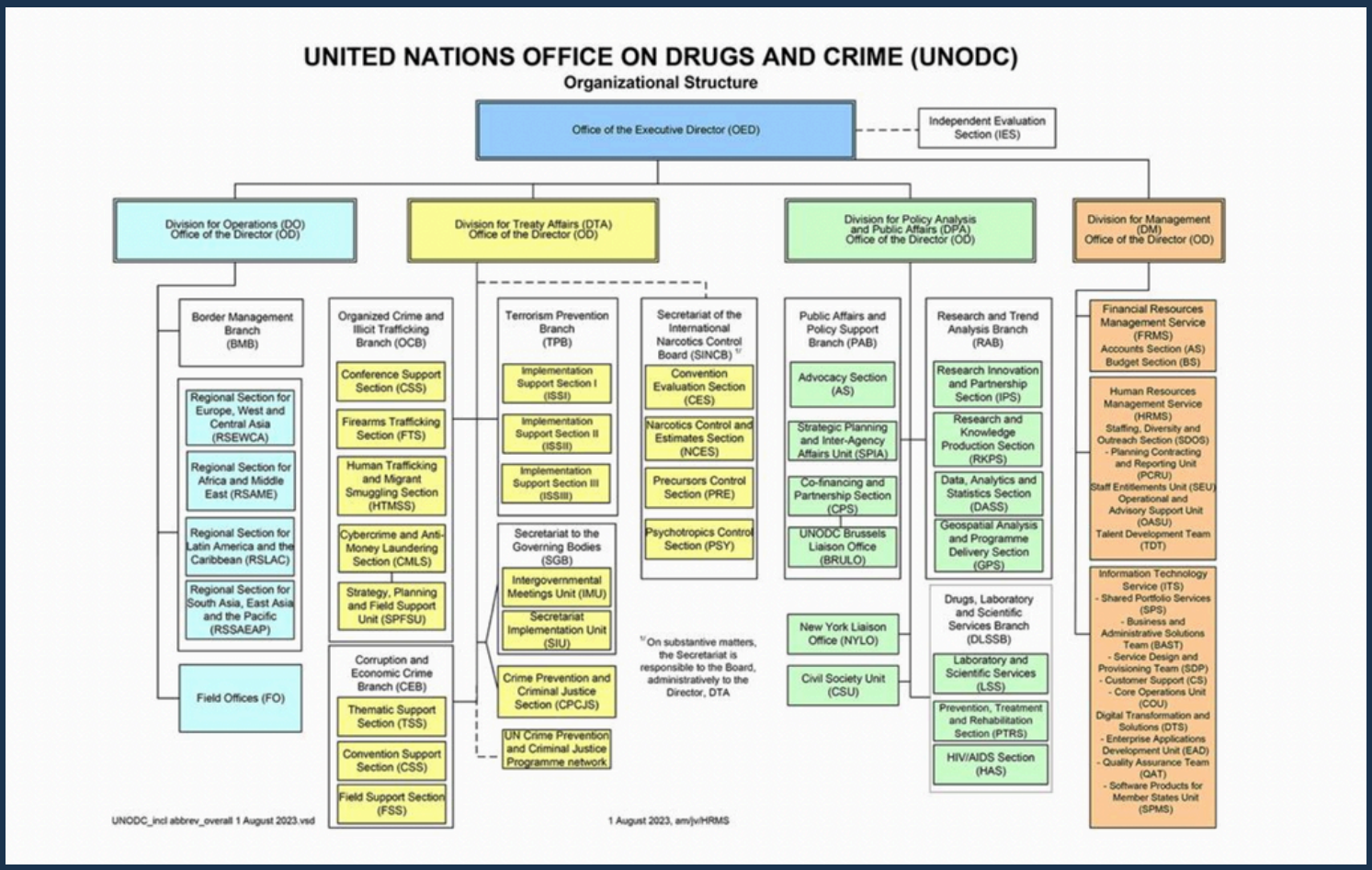
The UNODC provides technical assistance, research, and normative support to Member States to help them develop and implement comprehensive, evidence-based solutions to the complex and interconnected threats that they face at the national, regional, and global levels. Headquartered in Vienna with a network of over 130 offices around the world, UNODC advances justice, health, and security to build resilient societies and improve everyday life for individuals, families, and communities around the globe.

The UNODC is a global leader in the fight against illicit drugs, transnational organized crime, terrorism, and corruption, and is the guardian of most of the related conventions, particularly:

- The United Nations Convention against Transnational Organized Crime and its three Protocols (against trafficking in persons, smuggling of migrants, and trafficking in firearms)
- The United Nations Convention against Corruption
- The International Drug Control Conventions

The UNODC was established in 1997 as a result of the merging of the United Nations Centre for International Crime Prevention and the United Nations International Drug Control Programme. It was established by the Secretary-General of the United Nations to enable the Organization to focus and enhance its capacity to address the interrelated issues of drug control, crime, and international terrorism in all its forms.

The diagram below provides a detailed breakup of the different organs of the UNODC. This is in no way meant to be an exhaustive breakup and delegates are expected to further research upon the organs of the UNODC in detail and understand the relevance of each sub-division of the UNODC to the agenda and how it tackles the issue at hand.



In general, the UNODC, through the UNODC Strategy 2021-25, seeks to achieve the following goals

- Tackling the world drug problem through balanced, evidence-based responses to address drug abuse and drug use disorders, as well as the production and trafficking of illicit drugs

- Preventing corruption by promoting integrity and good governance and helping recover stolen assets

- Countering terrorism through effective, accountable, and inclusive legal, crime prevention, and criminal justice measures in line with international norms and the UN Global Counter-Terrorism Strategy

- Combating organized crime by providing technical assistance and support and strengthening international cooperation to address organized criminal activity and all forms of trafficking

- Preventing crime and promoting criminal justice through human rights-based and victim-centered approaches that strengthen the rule of law and access to justice

UNODC
United Nations Office on Drugs and Crime

UNODC'S WORK IS BASED AROUND FIVE NORMATIVE AREAS OF ACTIVITY

Strengthening Member States' capacities to confront threats from TRANSNATIONAL ORGANIZED CRIME

HOW?
- By helping Member States ratify and implement the UN Convention against Transnational Organized Crime and its Protocols
- promoting evidence-based policies to counter transnational organised crime and disseminating good practices
- collecting and disseminating data, disaggregated by sex, for policy analysis
- helping fight trafficking of illicit drugs, weapons, counterfeit goods, cultural property, humans, wildlife and other natural resources through field-oriented projects and programmes
- addressing new and emerging forms of crime, such as cybercrime
- raising awareness for human trafficking's victims and of its impact on society through the Blue Heart Campaign

Countering TERRORISM

HOW?
- By helping Member States implement the 19 international legal instruments against terrorism and enhance their policy and legislative responses
- helping states cooperate with one another to implement terrorism prevention measures
- helping build the capacity of national criminal justice systems to effectively prevent and counter terrorism through field-oriented projects
- enhancing the provision of juvenile justice, effective prison management and rehab, and social reintegration to prevent terrorism

Tackling CORRUPTION and its catastrophic impact on societies

HOW?
- By helping Member States ratify and implement the UN Convention against Corruption and develop domestic legislation to prevent and counter corruption
- helping to criminalise 11 different corruption offenses
- enhancing international cooperation on extradition and mutual legal assistance
- helping states recover assets stolen by corrupt officials
- promoting good governance, integrity and transparency
- enhancing States' anti-corruption capacities through technical cooperation projects

Supporting Member States in implementing a balanced, comprehensive and evidence-based approach to the WORLD DRUG PROBLEM that addresses both supply and demand

HOW?
- By helping Member States implement the three major international drug control treaties , and develop policies consistent with them
- implementing drug use prevention strategies with Member States
- supporting drug dependence treatment, support, and rehabilitation
- ensuring access to controlled substances for medical purposes
- helping illicit drug farmers develop alternative sustainable livelihoods
- analyzing and reporting data on drug trafficking trends, including arrests, seizures, price and purity of illicit drugs, to increase knowledge and promote evidence-based programming

Strengthening crime prevention and building effective CRIMINAL JUSTICE SYSTEMS

HOW?
- By boosting the rule of law and reinforcing human rights through implementing the United Nations Standards and Norms in Crime Prevention and Criminal Justice
- supporting UN standards promoting comprehensive crime prevention strategies and effective, fair and humane criminal justice systems, with a focus on specific challenges such as violence against women and children
- helping reform criminal justice structures and prisons through field-oriented technical cooperation
- providing States with sex-disaggregated data and analysis on key categories of violent crime, like homicide

In pursuing its objectives, UNODC makes systematic efforts to increase GENDER EQUALITY in order to ensure that men and women, boys and girls have equal access to rights, resources and opportunities.

It also enlists the support of GOODWILL AMBASSADORS to amplify its messages, such as Nadia Murad, Nobel Peace Prize laureate and UNODC Goodwill Ambassador for the Dignity of Survivors of Human Trafficking.

Introduction to the Agenda

Regulating the Illegal Use of Emerging & Existing Information and Communication Technologies on Curbing & Countering Criminal Activities

I. Overview

The rapid development of Information and Communications Technology (ICT) over recent years has resulted in the recent migration of Organized Crime and Terrorist Networks to the cyber domain with the consequent introduction of new cybercrime scenarios. As a result, the dimensions of criminal activities have become wider and more challenging from an investigative point of view. This section aims to provide an overview of the role of ICT in the context of organized cybercrime and terrorist networks by highlighting emergent scenarios that have been enabled. ICT, while having enormous potential for the development of States, creates new opportunities for perpetrators and may contribute to a rise in the levels and complexity of crime. There is a notable increase in the rate and diversity of crimes committed in the digital world and their impact on the stability of critical infrastructure of States and enterprises and on the well-being of individuals. There is a potential risk of the misuse of emerging technologies, including artificial intelligence, while recognizing their potential in preventing and combating the use of information and communications technologies for criminal purposes

There is no generally acceptable international definition or legal standard of what constitutes a cybercrime or cyberattack at the date of the creation of this Background Guide. Offenses typically cluster around the following categories:
i) offenses against the confidentiality, integrity, and availability of computer data and systems
ii) computer-related offenses
iii) content-related offenses
iv) offenses related to infringements of copyright and related rights
Broadly, cybercrime can be described as having cyber-dependent offenses and/or cyberenabled offenses

- Cyber-dependent crime requires an ICT infrastructure and is often typified as the creation, dissemination, and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power plant by an organized crime group), and taking a website offline by overloading it with data (for instance, a DDOS attack)

- Cyber-enabled crime is that which can occur in the offline world but can also be facilitated by ICT. This typically includes online fraud, purchases of contraband substances and illegal drugs online (for instance, via the Darknet/Deep Web), and online money laundering. What most people see online is only a small portion of the data that's out there on the 'clearnet'. Most search engines, for example, only index 4% of the internet. The Deep Web, which is defined as a part of the World Wide Web that is not discoverable by search engines, includes password-protected information – from social networks through to email servers.

The Darknet is a collection of thousands of websites that use anonymity tools like TOR to encrypt their traffic and hide their IP addresses. The high level of anonymity in the digital space enables criminals to act without being easily detected. The darknet is most known for blackmarket weapon sales, drug sales, and child abuse streaming. The darknet is also, however, used for good – including enabling free speech by human rights activists and journalists. Note: The current simulation of our Committee is premised on the workings of the Sixth Session of the proceedings of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes. Keeping in mind the relevance and requirements of the Committee, our primary focus is on cybercrime against individuals and not on cyber-terrorism.

1. Use of Artificial Intelligence in modern and contemporary criminal activities

The rapid advancements in the field of Artificial Intelligence ("AI") or Machine Learning ("ML") have brought about a massive revolution in the field of ICT. While AI is starting to make its way through all avenues and sectors of the world including law enforcement, it has also proved to be a double-edged sword proving to be a powerful tool for modern-day criminals, turning into a credible risk. [1]

In the realm of high threat severity, several concerning issues pose substantial risks to security. Among them, audio/video impersonation stands out, as it can be utilized for fraud, extortion, damaging reputations, or breaching security.

---

[1] **https://www.ojp.gov/pdffiles1/nij/252038.pdf**

The potential use of driverless vehicles as another alarming threat, with implications for public safety. Tailored phishing, exploiting trust relationships through highly personal data, and the disruption of AI-controlled systems in critical areas such as food logistics, public utilities, and traffic control add to the high-threat landscape. Large-scale blackmail leveraging harmful information from various sources and the creation of AI-authored fake news further amplify the severity of potential risks.

Moving to a medium threat security level, concerns include military robots, learning-based cyber attacks, and autonomous attack drones capable of independent action. The issue of 'snake oil' refers to fraudulent services falsely presented as genuine uses of AI or machine learning, while data poisoning involves manipulating data accessible to AI and machine learning systems. Online eviction, face recognition trickery, and market bombing in financial markets also fall into this intermediate threat category, demanding vigilant cybersecurity measures. Finally, at the low-threat security level, potential risks include the exploitation of bias, burglar bots infiltrating premises, evading AI detection techniques, and AI-authored fake reviews. AIassisted stalking via social media or cell phones, as well as AI-generated forgery attributed to known human authors, are also identified as potential low-level threats, underscoring the diverse challenges in maintaining security across various domains.
These threats that are posed by the advent of AI can only be curbed by implementing legislations that thoroughly examine the possibility of misuse of AI for the purpose of criminal activities and put in place reasonable restrictions limiting the possibility of misuse of AI for the same. A risk-based approach can be taken for the same to narrow down the most dangerous uses of AI and regulate/ban the same to prevent their misuse [2]

---

[2] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

2. Dark Web and its significance

The Internet has revolutionized the way people communicate, due to its ease of use. At the core of this lie search engines such as Google and Yahoo, which essentially catalog and arrange the most relevant information that is available on the internet. However, a large part of the Internet is not accessible to these search engines and stays hidden from the layman. The accessible part of the internet is termed the 'Surface Web' and this includes most social media, news, e-commerce websites, and others. The remainder which is hidden from the view of the public, is termed the 'Deep Web'. These webpages may be commercialized, such as in the case of commercial databases, or paid service websites, or may be part of an organization's Internal Network or Intranet. However, there is also a certain section of the "Deep Web" that is intentionally hidden behind layers of encryption and/or obscuring, which are used by individuals to conduct highly illegal activities. This is known as the "Dark Web" .[3]

Although the terms "Deep Web" and "Dark Web" are used highly interchangeably, they are very distinct. In recent years, the use of the Dark Web by criminal organizations has skyrocketed. The primary reason for this is the Anonymity provided by such a service, both to the end user and the service provider. The Dark Web as a tool has been used by several nefarious individuals and also by Organised Criminal Syndicates, and has been used as a tool for the illicit trade of narcotics, human trafficking, illegal trade of firearms, contract killing, and other such activities. The anonymity provided by the TOR interface has led to a certain level of difficulty in tracking and locating the servers hosting such websites, as well as in ascertaining the identity of the people operating these websites.

---

[3] https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=Some%20of%20the%20more%20prevalent,and%20other%20types%20of%20abuse

As a consequence of the increasing use of anonymization technology, illicit darknet marketplaces have become more accessible and popular. After Bitcoin was introduced in 2009, it was quickly adopted as a payment method in dark markets. Most notably, in 2011, the Silk Road market, an onion website providing a platform for buying and selling illegal products (mostly drugs), began to operate inside the Tor network using Bitcoin as its primary payment method (although today the use of privacy coins, such as Monero and Ethereum is increasing). Silk Road was the first time these technologies were combined to enable an online market for illegal products to grow significantly[4]. These marketplaces have not invented new technologies but rather combined various innovations that drive new benefits for both sellers and buyers.

Cryptocurrencies, due to their broad anonymity, have become the means for financing cybercrime on the dark web.

Law enforcement is getting better at taking down darknet markets, but that does not necessarily translate into fewer users/sellers. When a market is taken down, sellers and buyers usually transition to the next largest market. Sellers have even been observed operating under the same username as they move to other marketplaces; for example, starting on Silk Road, then moving to AlphaBay, and then onto more recent iterations. This shows that disruption does not necessarily solve the problem.

---

[4] https://pubmed.ncbi.nlm.nih.gov/25681266/

3. Money Laundering & Financial Crime

Money laundering, the process of obscuring the origins of unlawfully acquired funds through intricate financial maneuvers, faces both challenges and countermeasures in the era of ICT. [5] The digitization of financial transactions leaves a trail of digital footprints, empowering authorities to trace funds and identify suspicious activities. Advanced algorithms enable realtime transaction monitoring, swiftly detecting unusual or large transfers that may indicate money laundering. The integration of big data and artificial intelligence allows for rapid analysis of financial data, unveiling patterns, and irregularities, even within complex transactions

Blockchain technology contributes to the fight against money laundering by establishing transparent and tamper-resistant transaction records, preventing manipulative efforts by illicit actors. Online services leveraging digital identity verification protocols discourage the use of false identities for illegal transactions. Additionally, robust cybersecurity measures safeguard against cyberattacks that could facilitate money laundering activities. [6] The global nature of ICT fosters international cooperation among law enforcement and financial institutions, facilitating cross-border tracking and apprehension of money launderers. The rise of digital currencies, including cryptocurrencies, often favored by money launderers, is met with evolving regulations as blockchain's traceability challenges the misconception of complete anonymity. Machine learning and artificial intelligence technologies play a crucial role in recognizing intricate money laundering patterns, continuously improving their efficacy over time.

---

[5] https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html

[6] https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

Furthermore, the streamlined process of reporting suspicious transactions, facilitated by ICT, imposes reporting obligations on financial institutions, enhancing the overall resilience of the financial system against illicit activities.

4. Data Theft/Data Breach

Cybercrimes, also known as cyber-dependent crimes, mainly target systems, networks, and data with the intention of undermining their confidentiality (i.e., protecting systems, networks, and data so that only authorized users can access them), integrity (i.e., ensuring that data is reliable and accurate and has not been altered), and availability (i.e., making data, services, and systems available whenever needed). Hacking, virus production, acquisition, and dissemination, distributed denial of service (DDoS) and denial of service (DoS) attacks, and website defacement (a type of online vandalism that targets website content) are some examples of these cybercrimes. In order to harm the target, hackers may also attempt to gain unauthorized access to systems. In 2014, Lauri Love, a British hacker, vandalized websites, got unauthorized access to United States Government systems and stole valuable data from these systems. Due to unauthorized access to the website and system and information theft, this cybercrime jeopardized both the confidentiality and integrity of the data (by defacing web pages). [7]

[7] https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

5. 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. The traffickers often use violence or fraudulent employment agencies and fake promises of education and job opportunities to trick and coerce their victims.

The crime of human trafficking consists of three core elements: the act, the means, the purpose.

The Act:

To constitute the act of human trafficking the trafficker must do one of the following to the people – recruit, transport, transfer, harbor or / and receive

Means:

using one or more of these methods - threat or use of force, coercion, fraud, deception, abuse of a position of vulnerability, giving payments or benefits, abduction. Physical and sexual abuse, blackmail, emotional manipulation, and the removal of official documents are often used by traffickers to control their victims.

Purpose:

For exploitation Exploitation can take place in a victim's home country, during migration or in a foreign country

The UN Protocol to Prevent, Suppress, and Punish Trafficking[8] serves as the primary legal instrument to combat human trafficking . The protocol was adopted by the United Nations in November 2000 as part of the United Nations Convention against Transnational Organized Crime. It is the first legally binding instrument with an internationally recognized definition of human trafficking. This definition provides a vital tool for the identification of victims, whether men, women, or children, and for the detection of all forms of exploitation which constitute human trafficking. Countries that ratify this treaty must criminalize human trafficking and develop anti-trafficking laws in line with the Protocol's legal provisions.

6. Attack on digital infrastructure

From the perspective of the United Nations Office on Drugs and Crime (UNODC), an "attack on digital infrastructure" refers to any malicious activity aimed at disrupting, damaging, or gaining unauthorized access to information and communications technology (ICT) systems.

The effects of attacks on digital infrastructure are profound and far-reaching. Economically, cyberattacks can lead to significant financial losses for businesses, disrupt markets, and undermine investor confidence. For instance, ransomware attacks that lock users out of their data until a ransom is paid can cripple critical services in healthcare, finance, and other essential sectors.

---

[8] https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons

Politically, cyberattacks pose a huge risk to national security as they can expose classified information, disrupt military operations, and weaken defense mechanisms. State-sponsored cyberattacks can lead to espionage, the manipulation of public opinion, and public unrest as a response to its effects. Socially, such attacks can erode trust in digital systems, infringe on privacy, and expose individuals to identity theft and fraud. The global scale of these threats underscores the necessity for robust international cooperation and comprehensive legal frameworks to combat cybercrime effectively.

An attack on digital infrastructure encompasses a wide range of malicious activities targeting the systems, networks, and devices that support digital communication and data processing. These attacks can manifest in several ways:

1. **Illegal Interception:** This involves unauthorized access to non-public transmissions of digital information. Attackers intercept data as it travels across networks, which can lead to the theft of sensitive information, including governmental communications, personal data, and intellectual property. This kind of attack can undermine national security, disrupt governmental operations, and compromise the integrity of critical information.

2. Data Breaches: Unauthorized access to and extraction of confidential data from digital systems. Governments often store vast amounts of sensitive information, ranging from citizens' personal data to classified intelligence. Breaches can result in significant data loss, identity theft, and a loss of public trust in governmental institutions.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: These attacks aim to overwhelm systems with excessive traffic, rendering them inoperable. For governments, DDoS attacks can cripple essential services such as healthcare, emergency services, and public administration systems, causing widespread disruption and panic.

4. Ransomware: A type of malicious software that encrypts the victim's data, demanding a ransom to restore access. When targeted at government systems, ransomware can halt the functioning of public services, compromise sensitive data, and lead to significant financial losses. Governments may face difficult decisions regarding paying ransoms versus restoring systems independently.

5. Cyber Espionage: State-sponsored actors infiltrate government systems to steal confidential information for strategic advantages. This form of cyberattack threatens national security, diplomatic relations, and economic stability. Cyber espionage can provide adversaries with critical intelligence, undermining a nation's defense capabilities and political strategies.

6. Infrastructure Sabotage: Direct attacks on critical infrastructure such as power grids, water supplies, and transportation networks through cyber means. Such attacks can cause physical damage, endanger public safety, and disrupt daily life. Governments must invest in securing these infrastructures to prevent catastrophic consequences.

7. Disinformation Campaigns: Using digital platforms to spread false information and influence public opinion. These campaigns can erode trust in government institutions, manipulate electoral outcomes, and destabilize societies. Digital attacks aimed at sowing discord and confusion represent a significant challenge for maintaining public order and democratic integrity.

Delegates should explore existing international legislations, conventions, and protocols, such as the Budapest Convention on Cybercrime, the UN General Assembly Resolution 74/247[9] on Countering the Use of Information and Communications Technologies for Criminal Purposes, and the newly proposed Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

For research and further understanding, participants are encouraged to utilize resources from the UNODC Cybercrime Repository,[10] the Council of Europe's resources on the Budapest Convention[11], and the latest reports and guidelines from the International Telecommunication Union (ITU). By focusing on these areas, delegates can develop comprehensive strategies that address the multifaceted nature of digital infrastructure attacks and contribute to a safer, more secure digital world.

---

[9] https://undocs.org/A/Res/74/247

[10] https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

[11] https://www.coe.int/en/web/cybercrime/the-budapest-convention

7. Identity theft and social engineering

Identity theft involves the unauthorized acquisition and use of someone's personal information, typically for financial gain. Criminals may steal identities through various means, including hacking, phishing, and data breaches. The consequences for victims can be severe, ranging from financial loss to damaged credit scores and reputational harm.

Social engineering refers to the manipulation of individuals into divulging confidential information. Unlike traditional cyberattacks that exploit technical vulnerabilities, social engineering exploits human psychology. Techniques include phishing emails, pretexting, baiting, and tailgating. These methods often serve as precursors to identity theft, facilitating unauthorized access to sensitive information.

There exists a lack of precise and uniform definition regarding Identity crime. Not even the term used to describe the phenomenon is used consistently. While most United States publications use the term “identity theft”, the term “identity fraud” is very popular in the United Kingdom. Other terms used are for example “identity-related offences”, “phishing”, “account takeover” or “account hijacking”.

Although the lack of a precise definition generally does not impede the development of effective legal measures, it leads to two main issues. First, it complicates identifying the true extent of the problem, as diverse definitions make survey results difficult to compare. Second, without an agreed-upon definition, creating a coordinated international approach and conducting international investigations is more challenging.

Common or converged definitions are crucial for international cooperation, including transborder evidence sharing, extradition of offenders, and mutual legal assistance.

A few simplified definitions of identity related crime include:
a. Combining, obtaining and using an identity: Identity theft occurs when someone obtains another person's data or documents and then pretends to be that person. It requires both obtaining the information and using it to impersonate the victim.

b. Punishable act where identity is either a target or a tool: Identity-related crime includes all punishable activities involving identity as either the target or the main tool. This broad definition helps consider various identity-related offenses but is not precise enough for legal provisions.

c. Fraud or other unlawful activity where identity is either a target or tool: Identity theft involves using someone else's identity for fraud or other illegal activities without their consent. It focuses on identity and unlawful acts but lacks detailed descriptions.

d. Assumption of an identity: Identity theft can involve stealing or assuming an existing identity, whether the person is alive or dead. This definition emphasizes obtaining the identity but does not cover transferring or using the information.

e. Taking over a fictious identity or adopting the name of a person: ID fraud occurs when someone adopts a fictitious or real name without consent. It includes using pseudonyms and highlights that many identity thefts involve fake identities, though it primarily focuses on names.

8. Child sexual abuse and sexual exploitation

From the perspective of the United Nations Office on Drugs and Crime (UNODC), child sexual abuse and sexual exploitation refer to any activities that involve a child in sexual acts or the production of sexual content without their consent, often for the benefit of an adult. This includes a wide array of heinous acts such as child pornography, online solicitation, trafficking for sexual purposes, and sexual exploitation in travel and tourism. The rise of the internet and digital technologies has exacerbated these issues, making it easier for perpetrators to exploit children remotely and anonymously.

The effects of child sexual abuse and sexual exploitation are devastating and long-lasting, affecting not only the victims but also their families and communities. Victims often suffer severe psychological trauma, including depression, anxiety, and post-traumatic stress disorder. They may also experience physical health issues and face significant social stigmatization.

Addressing child sexual abuse and exploitation requires a comprehensive and multi-faceted approach. Delegates should focus on several key areas to effectively tackle this issue. Strengthening legal frameworks is of paramount importance when it comes to eradicating such heinous crimes. Legal challenges in responding to child sexual exploitation include problems related to insufficient legal coverage and consistency, and problems related to implementation. Projects such as UN-ACT (formerly UNIAP) [12] have made great strides in improving harmonization and legal cooperation between countries, but there is still much more work that needs to be done.

---

[12] https://erc.undp.org/evaluation/documents/download/2358

Delegates should explore existing international legislation and protocols, such as the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, child prostitution, and child pornography, and the Lanzarote Convention.

In the context of such horrific crimes that inflict severe psychological and physical trauma on victims, the adage "prevention is better than cure" is particularly apt. Preventive measures, such as public awareness campaigns and education programs that inform children, parents, and communities about the risks and signs of exploitation are essential. Protecting children in the digital age requires robust cybersecurity measures and partnerships with technology companies to detect and remove abusive content swiftly. Moreover, providing support services for victims, including psychological counseling and legal assistance, is vital for their recovery and reintegration into society. For further research, participants can utilize resources from the UNODC, the International Centre for Missing & Exploited Children (ICMEC), and the Global Partnership to End Violence Against Children.

Relevant Committees

FORMED UNDER AND ACTIONS TAKEN BY THE UN

1. Ad hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes[13]

The UNGA, in its 74th Session, decided to establish through its Resolution 274,[14] an openended ad hoc intergovernmental committee of experts, representative of all regions, to establish a comprehensive international convention on countering the use of information and communication technologies for criminal purposes, factoring in the existing international legal instruments[15] and the use of ICT for criminal purposes. Resolution 75/282, "Countering the use of information and communications technologies for criminal purposes," was adopted by the General Assembly on May 26, 2021.

The Ad Hoc Committee has met for six sessions, each lasting ten days, starting in January 2022 with a concluding session in New York. The General Assembly decided in the same resolution that the Committee would finish its work and present a draft convention to the Assembly at its seventy-eighth session. Additionally, the Committee follows the General Assembly's procedural rules and had held its first, third, and sixth negotiating sessions in New York and its second, fourth, and fifth sessions in Vienna.

---

[13] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[14] https://undocs.org/A/Res/74/247

[15] https://undocs.org/en/A/RES/75/282

2. Global Programme on Cybercrime [16]

UNODC's Global Programme on Cybercrime is a comprehensive initiative aimed at assisting member states in addressing various forms of cybercrime, including drug trafficking on the Dark Web. It includes efforts on the front of technical assistance, international cooperation in investigation, and the sharing of best practices. It has been set up in accordance with the Commission on Crime Prevention and Criminal Justice and has several aspects.

3. Budapest Convention [17]

The Budapest Convention, also known as the Convention on Cybercrime, is a global treaty aimed at tackling cybercrime and its growing threats. Established in 2001 by the Council of Europe, it's the first international agreement to address these issues. The Convention works in three key ways: harmonization, investigation, and cooperation. Member states agree to harmonize their national laws concerning specific cybercrimes like illegal access to computer systems, data forgery, and child sexual abuse online. This creates a consistent legal framework across borders, making it easier to prosecute cybercriminals who operate internationally. Additionally, the Convention outlines investigative techniques and procedures for gathering electronic evidence, which is crucial in the digital age. Finally, it fosters international cooperation by establishing channels for sharing information, providing mutual legal assistance, and facilitating fast and reliable extradition of cybercrime perpetrators.

---

[16] https://www.unodc.org/unodc/en/cybercrime/home.html

[17] https://www.coe.int/en/web/cybercrime/the-budapest-convention

4. Global Programme against Money Laundering[18]

The Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism("GPML") is a global programme established under the UNODC to provide in-depth assistance to member nations to strengthen their measures on anti-money laundering ("AML") and counter-terrorist financing measures ("CFT"). GPML, pursuant to multiple resolutions passed by the UNGA is tasked to, "continue providing technical assistance to Member States to combat money laundering and the financing of terrorism in accordance with United Nations related instruments and internationally accepted standards, including, where applicable, recommendations of relevant intergovernmental bodies, inter alia, the Financial Action Task Force on Money Laundering, and relevant initiatives of regional, interregional and multilateral organizations against money laundering."[17]

5. Financial Action Task Force[19]

New technologies have the potential to make AML/CTF decisions and measures faster, cheaper, and more effective. They can improve the implementation of FATF Standards to advance global AML/CFT efforts, ensure financial inclusion, and avoid unintended consequences such as financial exclusion.[20]

---

[18] https://www.unodc.org/unodc/es/money-laundering/global-programme-against-money-laundering/.html

[19] https://www.fatf-gafi.org/en/home.html

[20] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

III Relevant international standards and national regulations

1. GDPR [21]

The General Data Protection Regulation (GDPR) is a regulation in EU law on data privacy and protection for all individuals within the European Union (EU) and the European Economic Area (EEA). It essentially strengthens the control EU citizens have over their personal data and holds organizations accountable for how they collect, use, and store this information. The GDPR is important for several reasons. First, it grants individuals a range of rights, including the right to access, rectify, or erase their data. This empowers citizens to have more control over their digital footprint. Second, the regulation applies to any organization processing the data of EU residents, regardless of the organization's location. This creates a global standard for data protection. Finally, the GDPR includes hefty fines for non-compliance, ensuring organizations take data privacy seriously.

While the GDPR doesn't have direct jurisdiction over extradition, it does impact how data can be transferred outside the EU/EEA. The regulation outlines strict guidelines for ensuring the receiving country has adequate data protection measures. Organizations must also obtain clear consent for such transfers. The GDPR lays out a framework for lawful processing activities, requiring transparency and a legitimate reason for collecting data. It also defines important terms like "data subject" (the individual whose data is processed) and "data controller" (the organization responsible for data processing). These definitions are crucial for understanding rights and obligations under the regulation.

---

[21] https://gdpr-info.eu/

2. ISO 27001:2022 [22]

ISO 27001:2022 is the international standard for information security management systems (ISMS). It provides a framework for organizations to implement best practices for protecting their confidential information. Here's why it's crucial for information security:

- Systematic Approach: ISO 27001 isn't just a checklist; it guides organizations to establish a structured ISMS. This involves risk assessment, policy creation, and implementing controls to address vulnerabilities. This systematic approach ensures a holistic information security posture.

- Reduced Cyber Attack Risk: By identifying and addressing weaknesses, ISO 27001 helps organizations proactively mitigate cyber threats. The standard emphasizes controls like access controls, data encryption, and incident response planning, making it harder for attackers to infiltrate systems and steal data.

- Enhanced Security Posture: Implementing ISO 27001 strengthens an organization's overall security posture. It ensures consistent information security practices across departments, minimizes human error, and promotes a culture of security awareness within the organization.

---

[22] https://www.iso.org/standard/27001

3. ISO 27701:2019 [23]

ISO/IEC 27701:2019, also known as ISO 27701, is an international standard that builds upon the foundation of ISO 27001 (Information Security Management Systems) to provide specific guidance for protecting Personally Identifiable Information (PII). It essentially establishes a framework for organizations to implement a Privacy Information Management System (PIMS).
ISO 27701 is designed to complement ISO 27001. Here's a breakdown of its key aspects:

- Privacy-Specific Controls: The standard introduces additional controls specifically focused on privacy protection. These controls address areas like data subject rights management, data breach notification, and privacy impact assessments.

- Integration with ISMS: ISO 27701 emphasizes integrating privacy controls with an existing information security management system (ISMS) established under ISO 27001. This creates a holistic approach to managing both information security and privacy risks.

- Accountability Framework: The standard outlines a framework for establishing roles and responsibilities related to privacy management within an organization. This ensures clear ownership and accountability for protecting PII.

- Data Lifecycle Management: ISO 27701 emphasizes the importance of managing PII throughout its lifecycle. This includes controls for data minimization, data retention, and secure disposal of personal information.

---

[23] https://www.iso.org/standard/71670.html

4. DPDPA [24]

The Digital Personal Data Protection Act (DPDPA) is a proposed legislation in India that aims to govern the processing of personal data in a digital format. It seeks to strike a balance between individual privacy rights and the need for innovation in the digital age. The DPDPA is expected to have extraterritorial application, meaning it could apply to the processing of personal data of Indian citizens even if it occurs outside of India. This is particularly relevant for multinational corporations. The Act proposes the establishment of a Data Protection Board responsible for overseeing the implementation and enforcement of the DPDPA. This board would have the power to investigate complaints, issue fines for non-compliance, and raise awareness about data privacy rights.

Key Features of the DPDPA:

- **Individual Rights:** The DPDPA empowers individuals with various rights regarding their personal data, including the right to access, rectify, erase, and restrict processing. This grants them more control over how their information is used.
- **Accountability for Organizations:** Data fiduciaries will be held accountable for the security and privacy of personal data they process. The Act mandates clear guidelines and consent mechanisms for data collection and processing.
- **Data Security Measures:** The DPDPA is expected to enforce stricter data security measures to prevent unauthorized access, breaches, and misuse of personal data.

---

[24] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

- **Consent Framework:** Clear and specific consent from data principals will likely be a cornerstone of the Act. Organizations will need to obtain informed and verifiable consent before processing personal data.
- **Data Localization Requirements:** The DPDPA might introduce data localization requirements, mandating certain categories of personal data to be stored within India. This could have implications for international data transfers.

5. PIPL [25]

The Personal Information Protection Law (PIPL), which came into effect in November 2021, is a significant development in China's data governance landscape. It aims to regulate the collection, storage, use, and transfer of personal information within China. The PIPL applies to organizations that process the personal information of individuals within China, regardless of the organization's location. This has implications for foreign companies operating in China.

The Cyberspace Administration of China (CAC) is the primary regulatory body responsible for overseeing the implementation and enforcement of the PIPL. The CAC has the power to investigate violations, issue fines, and suspend data processing activities.

[25] https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html

Key Features of the PIPL:

- **Individual Rights**: The PIPL grants individuals certain rights regarding their personal information, including the right to access, rectify, erase, and restrict processing. However, the scope of these rights may be narrower compared to regulations like the GDPR.
- **Accountability for Processors**: Personal data processors are held accountable for the security and privacy of personal information they handle. The PIPL mandates clear data protection measures and imposes compliance obligations.
- **Consent Framework**: While consent is a requirement for processing personal information, the PIPL allows for some exceptions. Organizations may be able to process data without explicit consent under specific circumstances, which could raise concerns about user control.
- **Data Security Measures**: The PIPL mandates that personal information be processed securely, with appropriate technical and organizational safeguards in place.

While both the PIPL and GDPR aim to protect personal information, there are some key differences. The GDPR generally offers broader individual rights and stricter requirements for consent compared to the PIPL. Additionally, the PIPL allows for some data localization requirements, which are not present in the GDPR.

6. EU AI Act[26]

The European Union's proposed Artificial Intelligence Act (AI Act) aims to establish a comprehensive regulatory framework for the development, deployment, and use of artificial intelligence within the bloc. This legislation seeks to balance the potential benefits of AI with the need to mitigate its risks.

The core of the AI Act lies in a risk-based approach. AI systems are categorized based on their potential to cause harm, with high-risk applications facing stricter regulations. These high-risk categories might include systems used in facial recognition, credit scoring, or autonomous vehicles. For such applications, the Act mandates robust development processes, clear human oversight, and stringent testing to ensure fairness, transparency, and accountability.

The AI Act also focuses on protecting fundamental rights. It prohibits AI systems that manipulate or discriminate against individuals, and mandates safeguards for user privacy and data protection. Additionally, the Act grants individuals the right to explanation from AI-powered decisions that impact them, allowing them to understand the reasoning behind automated outcomes. The EU AI Act, if enacted, would be a landmark piece of legislation. It seeks to foster responsible AI development and use, creating a foundation for trust and innovation within the European Union. By establishing clear legal guardrails, the Act aims to ensure that AI serves humanity while mitigating potential risks.

---

[26] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Case Studies

1. Data breach at Target

In December 2013, a critical data breach unfolded at Target, one of America's retail giants, right in the middle of the busy holiday shopping season. Hackers infiltrated Target's point-of-sale systems, compromising the personal and financial information of millions of customers. The attack originated from an unexpected source: Fazio Mechanical Services, an HVAC contractor working with Target.

Fazio's weak cybersecurity measures proved to be the chink in Target's armor. Hackers exploited a vulnerability in Fazio's system, infected it with malware, and gained access to a contractor portal hosted by Target. This lack of network segmentation, where different parts of a network are isolated to prevent breaches from spreading, allowed the attackers a foothold within Target's system.

Capitalizing on this initial access, the attackers employed a series of sophisticated techniques. They used stolen credentials and single sign-on vulnerabilities to gain administrator privileges. They deployed malware disguised as antivirus software and bypassed security measures to infiltrate the database. While credit card information itself was protected by PCI standards, the attackers managed to steal customer names, addresses, phone numbers, and email addresses, along with encrypted debit card PINs. The breach exposed the limitations of focusing solely on internal network security and highlighted the critical role of robust vendor security practices and supply chain risk management. The Target incident became a watershed moment, prompting stricter regulations and accelerating the adoption of chip-and-PIN technology in the US to enhance credit card security.

2. The Russian Laundromat

The Laundromat Scheme, a complex money laundering operation exposed in 2014, serves as a cautionary tale for nations grappling with financial crime. Shell companies and fabricated debts were used to funnel illicit funds through Moldova and into the European Union's financial system. The scheme exploited weaknesses in Moldovan courts and lax enforcement to create a veneer of legitimacy for billions of dollars in laundered money. This case highlights the vulnerabilities inherent in a globalized financial system. Weak legal frameworks in some countries can be exploited by criminals, while even strong regulations require consistent enforcement to be effective. The Laundromat Scheme also underscores the importance of international cooperation. National risk assessments that identify money laundering vulnerabilities and holistic AML reforms that target both public and private sectors are crucial. Finally, strengthening state institutions through legal reforms that combat corruption and enhance transparency are essential for building robust anti-money laundering frameworks.

3. Vietnamese Migrants in UK Cannabis Industry

In recent years, Vietnamese migration to the UK has seen a rise in students and undocumented lowskilled workers, particularly in sectors like restaurants and nail salons. This coincides with looser visa policies in Vietnam. However, the lack of legal channels for unskilled workers pushes many into precarious situations.
A more concerning trend is the involvement of Vietnamese criminal networks in the UK's cannabis industry. Their expertise in cultivation, coupled with a shift towards domestic production in the UK, has led them to dominate this multi-billion euro market.

These networks exploit undocumented Vietnamese migrants, forcing them to work as isolated "gardeners" in cannabis farms under harsh conditions.

This situation exposes the complexities of Vietnamese migration. Economic opportunities drive migration, but a lack of legal options fosters exploitation by criminal groups. Addressing the root causes of illegal migration, establishing legal pathways for low-skilled labor, and protecting vulnerable migrants are crucial for a comprehensive solution.

Questions a Resolution Must Answer(QARMA)

Although not exhaustive in nature, we would ideally expect the discussions and deliberations through the days of the Conference (and finally reflected in the Outcome Document of the Committee) to touch upon the following, namely:

1. What are the key areas that should be focused on primarily by the UNODC in recommendations made to the Ad-hoc Committee to elaborate on a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes?
2. What are the potential ways in which AI can be regulated to ensure the prevention of misuse of new and emerging technologies including but not limited to biometric software, vulnerability detection software, deepfakes, and generative AI tools, for criminal purposes?
3. In what ways can existing mechanisms and instruments on AML/CTF be revamped to account for the increasing use of ICT for purposes of money laundering?
4. How can UNODC facilitate collaboration between member states, international organizations, and the private sector to combat the misuse of ICT and further enable all stakeholders to stay up-to-date with the latest trends in criminal activities pertaining to ICT?
5. In what ways can UNODC actively collaborate with the public and private sectors to make ICT more resilient to data breaches and theft, preventing leakage of sensitive and personal data?

References and Research Links

- https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010- 2019/2013/CCPCJ/Resolution_22-8.pdf
- https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmentalexpert-group-meeting-on-cybercrime.html
- https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- https://sgp.fas.org/crs/misc/IF12172.pdf
- https://arxiv.org/ftp/arxiv/papers/2104/2104.07138.pdf
- https://www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf
- https://ies.keio.ac.jp/upload/20191125econo_Wolfbang_wp.pdf
- https://unctad.org/system/files/officialdocument/Cybercrime%20Nayelly%20Loya%20%28UNODC%29.pdf
- https://sherloc.unodc.org/cld/about-us/index.html
- https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challengesof-New-Technologies-for-AML-CFT.pdf.coredownload.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/OHCHR2.pdf
- https://www.unodc.org/unodc/es/money-laundering/global-programme-againstmoney-laundering/.html

- https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-darkwebkumar#:~:text=Some%20of%20the%20more%20prevalent,and%20other%20types%2 0of%20abuse.
- https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/euai-act-first-regulation-on-artificial-intelligence
- https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf
- https://www.imolin.org/pdf/imolin/11-86446_financial_instruments_appr.pdf
- https://www.jisem-journal.com/download/concerns-about-cybersecurity-theimplications-of-the-use-of-ict-for-citizens-and-companies-13226.pdf
- https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/ICC.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/202308_INTERPOL_Written_Contribution_-_UN_AHC_6th_Session.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/OHCHR1.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Human_Rights_Watch.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/World_Bank.pdf

- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/UNICEF.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Internet_Society.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Privacy_International.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Privacy_Intl_EFF.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Chatham_House.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/CyberPeace_Institute.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Cybersecurity-Tech-Accord.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/DB_Connect_.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/GITOC_UN_AHC_negotiations_Aug2023.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Global_Partners_Digital.pdf

- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/AISur_EN.pdf
- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submi ssions/Multi-stakeholders/Microsoft_Submission_-_AHC_Sixth_Substantive_Session.pdf