IASMUN
Background Guide

UNITED NATIONS OFFICE ON DRUGS AND CRIME

LETTER FROM THE CHAIRS

It is our utmost pleasure to speak to you as part of the United Nations Office on Drugs and Crime in the International Academic School Model United Nations (IASMUN) 2026.

We are delighted to welcome you to this committee and we aim at giving you the chance to participate in discussions that would be intellectually stimulating and at the same time fun. In light of all the global problems shaping the present world, the plea for endurance has never been more urgent than now at UNODC, a body that is part of the United Nations, for it continuously supports the resolution of these issues through the interaction of nations in collaboration that is advantageous for all involved.

The conference will discuss the opportunities and challenges associated with narrowly focused issues such as countering the global rise of cybercrime and the dark web economy and disrupting the global trade in illicit arms and digital weapons.

The delegates from your committee are supposed to not only evaluate and communicate about these issues, but also to come up with and push for solutions that are practical and workable and which are grounded on the principles of resilience, fairness, and brotherhood of nations. The background guide has been made for you to help in your understanding of the topics and it will also be the base for your research. Yet, we strongly recommend you to perform your own research, since this background guide should not be your only resource.

LETTER FROM THE CHAIRS

With that being said, we ask you to not only think creative and come along this trip with a smiling face. Resilience is requiring the capacity to flex, schedule, and think outside the box.

You are the next leaders, and you are the ones who can lead the conversations that will create collaboration and balance of opportunities for all future generations. Good luck in your arrangements, and have a good time during the experience.

Regards,

Head Chair: Dawoud Qandah

Co-Chair: Omar Elsayed

INTRODUCTION TO THE COMMITTEE

The United Nations Office on Drugs and Crime, or UNODC for short, is an important agency at the United Nations with the goal of addressing the issue of drug use, international crime, corruption, as well as terrorism. The general mandate that the organization operates under is the cooperation with the Member States in creating a safe and just society.

UNODC was established in 1997, and since then, it has always acted as a well-liked and trusted counterpart of the government, civil society organizations, law enforcement agencies, and international bodies. UNODC has facilitated a global framework for combined action against crime through the collaboration of nations on different issues such as the struggle against trafficking, building judicial and law enforcement capacities, response to corruption, and reducing demand for drugs.

The UNODC is known as the "custodian organization" of major international instruments, including the Convention against Transnational Organized Crime and the Convention against Corruption. This can be attributed to the fact that these instruments impact the agenda of the global criminal justice system. The core pillars that make up the activities of the UNODC are research, international cooperation, and technical assistance. This helps the Member States in "promoting the rule of law, protecting human rights, and delivering on the SDGs, in particular SDG 3, SDG 5, SDG 10, and SDG 16."

INTRODUCTION TO THE COMMITTEE

With operations across more than 80 countries, UNODC provides countries with strategic guidance and technical assistance to strengthen their capacity to prevent and respond to crime and to provide protective services to victims of crime. The ultimate goal of the UNODC is to promote a world where countries can enjoy a just and safe society free from exploitation and violence associated with organized crime.

AGENDA 1

"Countering the Global Rise of Cybercrime and the Dark Web Economy"

The first agenda relates to the rising danger of cybercrime as well as the dark web economy. Cybercrime has grown from being an isolated occurrence of hacking into an organized profession that poses a global danger. Ransomware attacks, data breaches, financial fraud, as well as stolen identities, have become a common phenomenon, which translates to economic losses. This, in turn, affects the level of trust in the online world.

A major factor contributing to the occurrence of such events is the growing dark web world that incorporates encrypted online spaces providing criminal elements with a significant degree of anonymity. The dark markets allow for the trading of illicit services and goods such as drugs, firearms, stolen information, forged documents, and sophisticated hacking services on a largely anonymous manner. The use of cryptocurrency and anonymity networks makes such markets difficult to investigate.

The borderless nature of cyberspace means that most cybercrimes are international in nature, resulting in loophopes in the laws and thereby prolonging the investigation procedures. Countries with underdeveloped cybersecurity frameworks are highly susceptible to cybercrime routes, as these countries act as entry or exit points for cybercrime networks. The impact of cybercrime is not only economic in nature, as it affects vital services such as healthcare services and transportation services.

AGENDA 1

"Countering the Global Rise of Cybercrime and the Dark Web Economy"

In order to tackle this issue, the following is required on an international scale that encourages cooperation, aligns cybercrime laws, improves surveillance and shutdown efforts for the Dark Web marketplaces, and strikes a balance between security and the protection of core digital freedoms. The delegations are expected to work on proposals that align enforcement and privacy, innovation and regulation, and national sovereignty and cooperation respectively.

KEY ISSUES:

1. Rapid Growth of the Dark Web Economy

Illicit marketplaces on the dark web continue to expand, facilitating the trade of malware kits, hacking tools, drugs, weapons, stolen data, and other illegal services.

2. Increasing Sophistication of Cybercriminal Networks

Cybercrime has shifted from individual actors to organized transnational networks that employ advanced technologies such as encryption, artificial intelligence, and automation to conceal and scale their operations.

3. Ransomware and Attacks on Critical Infrastructure

Hospitals, financial institutions, government systems, and energy grids have become prime targets for ransomware attacks, posing severe risks to economic stability and public safety.

AGENDA 1

4. Use of Cryptocurrencies for Illicit Transactions

Cryptocurrencies enable pseudonymous transactions, making it increasingly difficult to trace financial flows linked to cybercrime, money laundering, and terrorism financing.

5. Uneven Cybersecurity Capabilities Across States

Many developing countries lack sufficient technical infrastructure and trained personnel, creating vulnerabilities that cybercriminals readily exploit.

PAST RESOLUTIONS:

1. International Treaties & Conventions -

The Budapest Convention on Cybercrime (2001) introduced the first-ever international agreement that focuses on cybercrime and cooperation through the synchronization of national laws, improvement of the investigative process, and the transfer of evidence over borders. Among the issues the Convention deals with, hacking, ransomware, cyber fraud, and cyber abuse fall into a unified legislative framework for the countries involved. After the Convention, the Second Additional Protocol (2022) aims an even further step in the sphere of cross-border cooperation and facilitates the access of electronic evidence and the coordination of law-enforcement bodies, so the process of the investigation of international cybercrimes gets accelerated, and becomes even simpler and more effective.

AGENDA 1

2. UN Resolutions & Actions

- The resolutions of the UNGA regarding "Counteracting the Use of ICTs for Criminal Purposes" support the idea of countries needing a more robust legal framework in combating cybercrime while urging more extensive cooperation in order to effectively respond to the abuse of these technologies. In this respect, the UNODC Cybercrime Programme delivers legal, technical support as well as expert training in an attempt to help countries improve their skills in terms of investigation as well as advance in digital forensics in order to combat increasingly sophisticated online criminal organizations.

3. Global Law Enforcement Operations

- There is the INTERPOL Global Cybercrime Programme, which deals with coordinating global cyber investigations by facilitating the exchange of intelligence information among the various countries that form the organizational structure of INTERPOL, as well as assisting in global operations against individuals who make use of cyber technology. In this regard, the J-CAT, which is the Joint Cybercrime Action Taskforce of Europol, partners with the various national law enforcement agencies in investigating and dismantling global cyber gangs as well as dark web market operations. The success of global operations, such as that of Dark HunTor, the AlphaBay market in 2017, as well as the Hansa Market in the same year, demonstrated the massive impact of global law enforcement cooperation, which led to the demise of the major dark web markets engaged in the trade of drugs, guns, as well as malicious software.

AGENDA 1

4. Financial Regulations & Crypto Oversight

- By their cryptocurrency standards, the Financial Action Task Force (FATF) has created a kind of benchmark for the whole world that is a complete norm on the planet so that every cryptocurrency exchange platform is supported by high-quality Know Your Customer and Anti-Money Laundering services on their structures and platforms. In this way, the platforms must also be provided with a very stringent control mechanism for their activities and must be obligated to report and collaborate on tracing the flow of illicit currencies, which might be used for cybercrime and other illicit activities on the cyberspace and cyberworld platforms and structures on the internet and other similar platforms and structures on the planet. The strategy has been adopted by many countries and has made the national licensing and registration of the cryptocurrency exchanges compulsory for them so that their platforms and structures must work and comply with very strict guidelines and settings on the planet for eliminating anonymity on the currencies as well as making the cyber and financial atmosphere on the whole planet much safer and far more authentic on the planet

5. Cybersecurity in the Regions

- The EU Cybersecurity Act is a major step ahead in the harmonization of the cybersecurity standards on the entire territory of the EU. This is done by implementing a strict cybersecurity framework that all digital products and services in the EU are obliged to meet, and, of course, the implementation of the certification framework for the EU that will ensure the compliance of all EU states with the same cybersecurity standards.

AGENDA 1

4. Financial Regulations & Crypto Oversight

- By their cryptocurrency standards, the Financial Action Task Force (FATF) has created a kind of benchmark for the whole world that is a complete norm on the planet so that every cryptocurrency exchange platform is supported by high-quality Know Your Customer and Anti-Money Laundering services on their structures and platforms. In this way, the platforms must also be provided with a very stringent control mechanism for their activities and must be obligated to report and collaborate on tracing the flow of illicit currencies, which might be used for cybercrime and other illicit activities on the cyberspace and cyberworld platforms and structures on the internet and other similar platforms and structures on the planet. The strategy has been adopted by many countries and has made the national licensing and registration of the cryptocurrency exchanges compulsory for them so that their platforms and structures must work and comply with very strict guidelines and settings on the planet for eliminating anonymity on the currencies as well as making the cyber and financial atmosphere on the whole planet much safer and far more authentic on the planet

5. Cybersecurity in the Regions

- The EU Cybersecurity Act is a major step ahead in the harmonization of the cybersecurity standards on the entire territory of the EU. This is done by implementing a strict cybersecurity framework that all digital products and services in the EU are obliged to meet, and, of course, the implementation of the certification framework for the EU that will ensure the compliance of all EU states with the same cybersecurity standards.

AGENDA 1

In addition, the NATO Cooperative Cyber Defence Centre of Excellence is focused on support for research, training, and international exercises that aim at making the allied states' common capabilities against all cyber-attacks stronger and less vulnerable. In turn, the training, technical support, and advice offered within the framework of the Cyber Capacity Building Initiatives of the ASEAN help the member states' cybersecurity resilience gain strength, which will enable all of them to commonly struggle against all cyber dangers.

6. Capacity Building & Technical Assistance

- The establishment and development of the Computer Emergency Response Teams and Computer Incident Response Teams within various nations, especially among the nations where the UNODC and the INTERPOL extend support, has emerged as one of the most effective steps taken against cybercrimes. The cyber defense capabilities within the nations have improved remarkably because of this. International training in digital forensics and crypto tracking has helped law enforcement practitioners become responsive to recognize, prevent, and respond to cybercrimes

AGENDA 2

"Blood Circuits: Disrupting the Global Trade in Illicit Arms and Digital Weapons"

The second agenda concerns the intersection of arms trafficking and digital weaponization, which poses an increasingly significant threat to international peace and security. Traditional black market arms trafficking, which has for a long time been associated with armed conflicts, organized crime, or terrorism, is increasingly blurring with the business of cyber-based products such as malware, ransomware kits, spyware, or zero-day exploits.

The flow of physical weapons across unregulated borders persists, and the digital form of the same is being trafficked through the internet. These tools help in striking the electricity supply, the finance systems, the government data, and the essential services. The efficiency of these tools has increased because of the use of encrypted communications, cryptocurrencies, and the multiple routes available for smuggling.

In order to effectively counter the dual challenge posed, there is a need for holistic approaches that interfere with the physical as well as the virtual supply chain, the online marketplace, intelligence sharing, and the regulatory lacunae at the global and international levels respectively.

AGENDA 2

KEY ISSUES:

1. Convergence of Physical and Digital Weaponry

Illicit arms and cyber weapons are increasingly traded through the same networks, allowing criminals to coordinate operations more efficiently and evade detection.

2. Expansion of Dark Web Arms Markets

Anonymous online platforms facilitate the sale of small arms, digital attack tools, and dual-use technologies with limited accountability.

3. Weak International Tracking and Verification Systems

The absence of unified systems to track weapons and malware allows illicit goods to cross borders undetected and cyber threats to spread rapidly.

4. Complex Trafficking Logistics

Weapons trafficking now exploits air, sea, land, and postal services, significantly complicating monitoring and interdiction efforts.

5. Rise of DIY Weapons and Cyber Toolkits

Advances in 3D printing and downloadable exploit kits enable decentralized production with minimal oversight

AGENDA 2

PAST RESOLUTIONS:

1. United Nations Programme of Action on Small Arms and Light Weapons (PoA, 2001)

- The PoA has been put in place to manage the global distribution of small arms and light weapons, which are the main instigators of wars, organized crime, and widespread violence. It is a very good start for the development of countries in such areas as the management and security of their stockpiles, the establishment of national reporting mechanisms and the international cooperation for the tracking and prevention of the diversion of weapons into illicit markets. By means of promoting transparency, sharing of information, and following the best practices for arms management, the PoA is to lessen the impact of illegal weapons on the human and societal costs.

2. Arms Trade Treaty (ATT, 2014)

- The ATT stipulates rules that have the force of law for the global movement of conventional weapons, consisting of firearms, ammunition, and military hardware. Its main aim is to ensure that arms will not find their way into areas of warfare, terrorist organizations, or governments violating human rights. The treaty's mechanisms of transparency include mandatory state reporting, assessments of risk prior to export approvals, and facilitation of dialogue between the exporting and importing nations in order to minimize the amount of illegal arms flowing. The ATT establishes uniformity in regulation and thus fortifies worldwide accountability in the trade of arms.

AGENDA 2

PAST RESOLUTIONS:

3. Law-Enforcement Operations by INTERPOL and Europol
- INTERPOL and Europol have conducted a number of operations collectively that targeted the illegal arms trade, selling dual-use technologies, operating dark-web marketplaces, and dealing with malware and cyber tools. The international cooperation among law enforcement agencies resulted in arrests, the dismantling of crime groups, and seizure of illegal goods. The operations, which were based on the sharing of intelligence, resources, and expertise among several countries, serve as a powerful demonstration of the effectiveness of cooperation in the fight against both physical and digital illicit trade.

4. Regional Frameworks
- Arms export policies like the EU Common Position and programs of ASEAN Regional Forum are regional initiatives that allow member countries to cooperate on control over the monitoring, probing, and regulating of arms. The established frameworks allow for collaborative inquiries, provision of technical aid, and sharing of best practices in order to eliminate the illegal trade. Through the establishment of a regional partnership, these steps have been taken to support international treaties and resolutions, thus improving the capability of countries in unison to successfully curb the spread of illegal arms as well as digital weapons.

AGENDA 2

MAJOR PARTIES INVOLVED:

1. United States

The United States is considered to be the most vulnerable nation in terms of cyberattacks mainly because of its very advanced electronic economy and the great impact it has worldwide. It is where the large technology organizations, banks, and vital infrastructure systems are located, which makes it an easy target for ransomware and data theft. Furthermore, the U.S. has the most powerful cyber security and crime investigation units, namely FBI Cyber Division, NSA, and Cyber Command. It is a strong proponent of international collaboration, imposition of sanctions on cyber criminals, and prosecutions of dark web marketplaces.

2. Russia

Russia has frequently been associated with the very best and most classy cybercriminals that can be found all over the world; still, such a large number of them are said to be doing their business with almost no fear if they do not go after Russian citizens. Among the methods depicted as state-supported actors, cyber-espionage, ransomware, and disinformation campaigns are the most common ones. Though Russia has built up very powerful cyber resources, the argument over cyber ethics with the West is still around and this leads to conflicts at international talks.

3. China

China has become a major player in cyberspace, and has done so by pouring money into its cyber defense, surveillance and offensive capabilities. For many years, the Chinese hackers have been responsible for various activities, such as stealing of intellectual property, penetrating influential sectors, and causing outages in essential services in different parts of the globe.

AGENDA 2

MAJOR PARTIES INVOLVED:

it very often refuses to accept the West's approaches that prioritize transparency and attribution.

4. United Kingdom

Cybersecurity research and regulations in the UK have obtained worldwide recognition as their main source. Infrastructures like these are also subjected to constant cyberattacks, particularly in the financial and energy sectors, and government networks. The National Cyber Security Centre (NCSC) of the UK is making a very significant contribution to the worldwide battle against ransomware, improving digital resilience, and sharing the cost of international cybercrimes. The UK speaks out veraciously for tougher legislation on cybercrimes and for sharing of information across borders.

5. India

India has one of the largest digital populations in the world and online services that are growing very fast. Consequently, the country is facing a rise in cybercrime threats which involve financial fraud, identity theft, and hacking of government portals. India is not only strengthening its cybersecurity laws but is also cooperating with international law enforcement agencies. It is still lagging behind the developed nations in the area of cybersecurity skills but has made itself a top target for hackers and, at the same time, a needed ally in worldwide cyber partnership.

6. Germany Germany is a country that is often the target of cyber assaults that mainly focus on its industrial, financial, and governmental sectors, and is nevertheless considered one of the biggest economies in Europe. It vehemently advocates for privacy protections, EU-wide cyber regulations, and cooperation among law enforcement through Europol.

AGENDA 2

MAJOR PARTIES INVOLVED:

The German intelligence services play an active role in monitoring international cybercrime organizations and making the EU more digitally self-sufficient.

7. North Korea / DPRK

North Korea possesses the reputation of employing cybercrime as a primary source of income owing to the economic sanctions. Among the culprits, the Lazarus Group has been associated with several ransomware attacks, theft of cryptocurrency, and burglaries of banks around the globe. The North Korean government refutes its participation but still stands as one of the major cyber threats worldwide.

8. Japan

Japan's sophisticated tech ecosystem is attractive to hackers and cyber terrorists and hence, it becomes a target for such attacks in the areas of robots, production, and finances among others. Besides, it has started to develop the standards for international cybersecurity and constantly works with various organizations to follow the development of cybercriminal activities.

9. South Korea

The digital society of South Korea makes it open to attacks from the cyber world, especially from North Korean characters, which are often the case. The government is always investing a lot of money in cyber defense and at the same time operates very closely with international cybersecurity networks. The approach of South Korea in this area is much more focused on cyber resilience, fintech protection, and accretion of international communication.

AGENDA 2

Relevant Stakeholders Involved:

1. National Governments:

National governments have the duty to share responsibility for the enforcement of the laws regarding cybercrime, the regulation of firearms, and the protection of borders against the trafficking of illegal goods. They are the main actors in the uniting of law-enforcement, intelligence, and cybersecurity agencies to follow and break up criminal groups. Their efficiency is a key factor in determining both global cooperation and national preparedness in the case of weapon flows, whether they are physical or digital, and that is why their role is so crucial.

2. Law Enforcement Agencies:

Law enforcement agencies such as police, border patrol, customs, and intelligence units perform various activities across borders including arrests, online investigations, and monitoring the dark web. They also conduct raids, confiscate illegal arms, and follow the operations of cybercriminals. The extent of their collaboration and the level of their technological capabilities are the main factors that decide the effectiveness of I trafficking networks' disintegration.

3. Intergovernmental Organizations:

Organizations such as INTERPOL, UNODC, and Europol make it easier for the countries to work together globally by offering common databases, legal frameworks, and specific training. They connect different knowledge and information of the states and empower the states to react uniformly to crimes that cross borders. Their participation is very important, as the illegal trafficking activities very seldom happen entirely within the borders of one country.

AGENDA 2

Relevant Stakeholders Involved:

4. Computer Emergency Response Teams (CERTs):

CERTs support government agencies in identifying and removing malware, conducting digital forensics, and providing incident response to cyber attacks associated with digital weapons. Besides, they keep an eye on questionable cryptocurrency transactions and find out the dark web's most common exploit kits. Their technical know-how is extremely important for countries that have not developed strong cybersecurity solutions yet.

5. Internet platforms and technology companies:

Hosting, messaging, encryption, and telecom services offered by tech companies are pivotal in the detection of bad behavior and the elimination of unlawful content. They support the law enforcement agencies by marking the dubious accounts, notifying them about the cyberattacks, and making the platform security stronger. Their partnership is very important for the criminals' networks to be able to use this practice less.

6. Blockchain analysts and cryptocurrency exchanges:

By applying KYC/AML protocols, Exchanges have the authority to either block or report suspicious crypto transactions that may be involved in the illegal purchase of arms or malware, for instance. Moreover, companies engaged in blockchain analysis are the ones who follow and reveal the financial pathways of the dark web through the so-called anonymous transactions. These entities, in collaboration, manage to cut off the financial support of the illegal trade in arms, whether digital or physical, at their very core.

AGENDA 2

Relevant Stakeholders Involved:

7. NGOs and Civil Society:

NGOs take the initiative in creating public awareness, and they also are engaged in the promotion of digital safety, as well as supporting areas that are susceptible to crime-related recruitment. They provide the areas of research, policy advocacy, and victim assistance in connection with arms trafficking and cybercrime. By their local engagement, more ethical and people-centered solutions are already informed.

8. Terrorist Organisations and Organised Crime Groups:

The influential players in the illegal trade of arms and cyber weapons—primary consumers and distributors at the same time—are these entities. They are supplied with funds and made stronger by taking advantage of the dark web markets, ransomware, and smuggling routes. Therefore, the monitoring and disruption of their operations are very important to the global security risk reduction process.

KEY TERMS:

1. Cybercrime

The range of cybercrime includes a variety of illegal activities such as hacking, stealing of data, online scamming, and ransomware among others.

2. Dark Web

One can consider the dark web as the most clandestine area of the internet where no search engine can reach and only specially made software like Tor that keeps the user's identity hidden can enter. It has a bad reputation for being the home of digital black markets and illegal services.

AGENDA 2

Relevant Stakeholders Involved:

3. Deep Web

The deep web is that part of the Internet that nobody can see," It is claimed that only a small part of this deep web is illegal (like private emails, banking portals), and it is often mistaken for the dark web.

4. Dark Web

Economy The dark web economy is the minefield of illicit activities that are all hidden in the dark and their scale is still ambiguous, but they most likely cover the entire digital range from drug trafficking to selling hacked identities and even arm trade by means of digital transactions.

5. Ransomware

It is a software that either takes control to lock the user's access or encrypts the user's data and then demands a ransom (the payment is usually in cryptocurrencies) for unblocking the data access.

6. Malware

The word describes a broad category of malicious programs that come in various forms and might facilitate access to the system, causing disruption and even damage such as viruses, worms, Trojan horses, and spyware.

7. Phishing

It is a tricky cyber technique that uses fake emails or messages to lure people into giving out confidential information such as login credentials or bank details.

8. Encryption

It is a method of securing data that transforms the original data into a cryptic code. Although it is a necessity for security, it is also used by criminals to hide illegal activities.

AGENDA 2

Relevant Stakeholders Involved:

9. Cryptocurrency

The digital or virtual currencies (like Bitcoin) that all rely on cryptography are extremely controversial and very often linked to cybercrimes because of their feature of transactions that are either disguised or hard to trace.

10. Botnet

The very machines that a hacker has compromised and taken over are the ideal setups for carrying out large-scale attacks such as DDoS (Distributed Denial-of-Service) attacks).

11. Digital Forensics

The process of gathering, examining, and safeguarding electronic evidence for the purpose of identifying and prosecuting cybercrime offenders.

13. Anonymity Networks

Like Tor, to mask the user's identity and place. These services are widely used not only to secure privacy but also for illegitimate activities.

14. Transnational Organized Cybercrime

The hacker networks that operate across international borders and, consequently, the cooperation of countries through international channels is a necessity for both the investigation and prosecution of such crimes.

15. Illicit Arms

Trafficking The illegal trading and distribution of weaponry, including small arms, light weapons ammunition, explosives, etc.

16. Exploit kits

Downloadable software packages that include tools that are used to start cyberattacks.

AGENDA 2

Relevant Stakeholders Involved:

17. Supply Chain Diversification The use of multiple ways to illegally transport items without being easily detected, like sea, air, land.

QUESTIONS TO CONSIDER:

AGENDA 1:

1. To what extent can governments monitor encrypted networks while protecting civil liberties, freedom of expression, and digital privacy?
2. How should international legal frameworks be strengthened to prosecute cybercriminals operating across jurisdictions?
3. How can governments counter adaptive cybercriminal networks without displacing them into less traceable platforms?
4. What strategies can enhance national cyber resilience against ransomware, AI-driven cybercrime, and supply-chain attacks?
5. How effective are long-term measures such as education, awareness campaigns, and capacity-building in reducing cybercrime?

AGENDA 2:

6. How far should states go in monitoring encrypted platforms linked to cyber-enabled arms trafficking without violating fundamental rights?
7. What international legal instruments are required to address cyber-enabled arms trafficking across jurisdictions?
8. How can states adapt to decentralized and peer-to-peer trafficking networks without exacerbating enforcement challenges?
9. What actions can strengthen resilience against cyber-enabled arms purchases and attacks on customs and port systems?
10. How can long-term prevention strategies reduce the operational space of cyber-enabled arms trafficking?

BIBLIOGRAPHY

AGENDA 1:

Financial Action Task Force. (2021). Updated guidance for a risk based approach to virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021 .html

INTERPOL. (2023). Cybercrime. INTERPOL. https://www.interpol.int/en/Crimes/Cybercrime

United Nations Interregional Crime and Justice Research Institute. (2024). Beneath the surface: Terrorist and violent extremist use of the dark web and cybercrime-as-a-service for cyber-attacks. https://www.un.org/counterterrorism/en/beneath-surface-terrorist-and-violent-extremist-use-darkweb-and-cybercrime-service-cyber-attacks

United Nations Office on Drugs and Crime. (2020). Darknet cybercrime threats to Southeast Asia: An introductory analysis of darknet-enabled threats against Southeast Asian countries. https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

United Nations. (2024). UN General Assembly adopts landmark convention on cybercrime. United Nations. https://egypt.un.org/en/286532-un-general-assembly-adopts-landmark-convention-cybercrime

AGENDA 2:

United Nations News - Illicit weapons fuelling conflicts worldwide https://news.un.org/en/story/2025/11/1166324

Atlas Institute for International Affairs - The Illicit Arms Trade https://atlasinstitute.org/the-illicit-arms-trade-forever-wars-in-the-global-south/ United Nations Office on Drugs and Crime - The Illicit Market in Firearms (PDF)

BIBLOGRAPHY

United Nations Office for Disarmament Affairs - Small Arms and Light Weapons
https://disarmament.unoda.org/en/our-work/conventional-arms/small-arms-and-light-weapons

INTERPOL. (2022). Illicit arms trafficking. INTERPOL.
https://www.interpol.int/en/Crimes/Illicit-arms-trafficking

Europol. (2021). Internet organised crime threat assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.
https://www.europol.europa.eu/iocta-report