Vedic International School MUN 2025

United Nations Office on Drugs and Crime

Background Guide

Agenda- Strengthening International Cooperation to dismantle Dark Web Markets for Illicit Drugs and Arms.

Contents:

1. Letter from the Executive Board

Greetings Delegates,

We are very pleased to welcome you to the simulation of the UNODC at Vedic International School MUN 2025. It will be an honour to serve on your Executive Board for the duration of the conference. This Background Guide is designed to give you an insight into the case at hand. Please refer to it carefully. Remember, a thorough understanding of the problem is the first step to solving it.

However, remember that **this Background Guide is in no way exhaustive and is only meant to provide you with enough background information to establish a platform for beginning the research**. Delegates are highly recommended to do a good amount of research beyond what is covered in the Guide. The guide cannot be used as proof during the committee proceedings under any circumstances.

Finally, we would like to wish you luck in your preparation. In case you have any questions, procedural or otherwise, please feel free to direct them to any member of the Executive Board and we will get back to you as soon as possible. Please do not hesitate to contact us with any queries or concerns. We expect all delegates to be well-versed with the various nuances of the agenda and geared up for an intense debate, deliberations, and great fun.

We are looking forward to meeting you at the conference!

All the Best

Executive Board | UNODC

Sai Preethi Polu - Chairperson (saipreethi.polu@gmail.com)

Devayush Das - Vice Chairperson (devayushdas@gmail.com)

2. Points to Remember

A few aspects that delegates should keep in mind while preparing:

1. **Procedure:** The purpose of putting in procedural rules in any committee is to ensure a more organized and efficient debate. The committee will follow the UNA-USA Rules of Procedure. Although the Executive Board shall be fairly strict with the Rules of Procedure, the discussion of the agenda will be the main priority. So, delegates are advised not to restrict their statements due to hesitation regarding the procedure.
2. **Foreign Policy:** Following the foreign policy of one's country is the most important aspect of a Model UN Conference. This is what essentially differentiates a Model UN from other debating formats. To violate one's foreign policy without adequate reason is one of the worst mistakes a delegate can make.
3. **Role of the Executive Board:** The Executive Board is appointed to facilitate debate. The committee shall decide the direction and flow of the debate. The delegates are the ones who constitute the committee and hence must be uninhibited while presenting their opinions/stance on any issue. However, the Executive Board may put forward questions and/or ask for clarifications at all points in time to further debate and test participants.
4. **Nature of Source/ Evidence:** This Background Guide is meant solely for research purposes and must not be cited as evidence to substantiate statements made during the conference. Evidence or proof for substantiating statements made during the formal debate is acceptable from the following sources:
    a. **United Nations:** Documents and findings by the United Nations or any related UN body are held as credible proof to support a claim or argument. Multilateral Organizations: Documents from international organizations like OIC, NAFTA, SAARC, BRICS, EU, ASEAN, the International Criminal Court, etc. may also be presented as credible sources of information.
    b. **Government Reports:** These reports can be used in a similar way as the State Operated News Agencies reports and can, in all circumstances, be denied by another country.
    c. News Sources:
        i. **Reuters:** Any Reuters article that clearly makes mention of the fact or is in contradiction of the fact being stated by a delegate in the council.
        ii. **State operated News Agencies:** These reports can be used in the support of or against the State that owns the News Agency. These reports, if credible or substantial enough, can be used in support of or against any country as such but in that situation, may be denied by any other country in the council. Some examples are – RIA Novosti (Russian Federation), Xinhua News Agency (People's Republic of China), etc.

*****Please Note:** Reports from NGOs working with UNESCO, UNICEF, and other UN bodies will be accepted. Under no circumstances will sources like Wikipedia, or newspapers like the Guardian, Times of India, etc. be accepted. However, notwithstanding the criteria for acceptance of sources and evidence, delegates are still free to quote/cite from any source as they deem fit as a part of their statements.

3. Introduction to the Committee

The UNODC is a programmatic body and does not host debates, making it unsuitable to simulate in a Model UN setting. Instead, its governing body, the Commission on Crime Prevention and Criminal Justice (CCPCJ), will be simulated to allow structured debate and policymaking. The Commission guides the activities of the United Nations in the field of crime prevention and criminal justice. It also reviews United Nations standards and norms in this area, including their use and application by Member States. It takes action through resolutions and decisions. Mandate and functions of CCPCJ are as follows:

Functional commission of the Economic and Social Council (ECOSOC): The Commission was created in 1992 by the Economic and Social Council as one of its functional commissions (resolution 1992/1), upon request of the General Assembly. The Council has established the Commission's mandates and priorities, which include international action to combat national and transnational crime, including organized crime, economic crime and money laundering; promoting the role of criminal law in protecting the environment; crime prevention in urban areas, including juvenile crime and violence; and improving the efficiency and fairness of criminal justice administration systems (resolution 1992/22).

Governing body of UNODC: The Commission acts as the governing body of the United Nations Office on Drugs and Crime. It approves the budget of the United Nations Crime Prevention and Criminal Fund, which provides resources for promoting technical assistance in the field of crime prevention and criminal justice worldwide.

United Nations Crime Congresses: The Commission provides substantive and organizational direction for the quinquennial United Nations Congress on Crime Prevention and Criminal Justice. It also considers the outcome of the congresses and takes decisions on appropriate follow-up measures.

Programme network of Institutes: The Commission also maintains links to the United Nations Crime Prevention and Criminal Justice Programme Network, which supports the efforts the United Nations in the area of crime prevention and criminal justice and contributes to the work of the Commission.

History: The political agreement to establish the Commission derived from a ministerial meeting held in Versailles in 1991. It was preceded by a more technically focused Committee on Crime Prevention and Control, formed in 1971 to replace an earlier expert advisory committee and tackle a broadened scope of UN interest in criminal justice policy.

4. Overview on the Agenda

The internet has fundamentally changed the way people live, work, and interact. Widespread access creates unprecedented connectivity and access to information. Driving innovation and economic growth. However, beyond this incredible progress, there is a more hidden and obscure side of the Internet: the Dark Web.

The dark web, a concealed portion of the internet not indexed by traditional search engines, has evolved into a hub for illicit activities, including data breaches, identity theft, and the trade of stolen business credentials. Unlike the surface web, which hosts public websites, and the deep web, which contains private databases and internal systems, the dark web is accessible only through specialised browsers like Tor. While originally designed to support anonymity and privacy, it has become increasingly exploited by cybercriminals.

For Small and Medium-Sized Businesses (SMBs), the dark web represents a persistent threat. Compromised employee credentials, leaked customer information, and exposed intellectual property often find their way into dark web marketplaces. These exposures can lead to severe financial and reputational consequences if left undetected. Consequently, cybersecurity for businesses, particularly SMBs, must now account for dark web monitoring and risk mitigation strategies as part of a broader security posture.

In response to these growing risks, law enforcement agencies worldwide are intensifying efforts to dismantle dark web networks. Through collaborative operations and advanced digital forensics, organisations such as the FBI and Europol are making tangible progress in cracking down on these hidden criminal ecosystems.

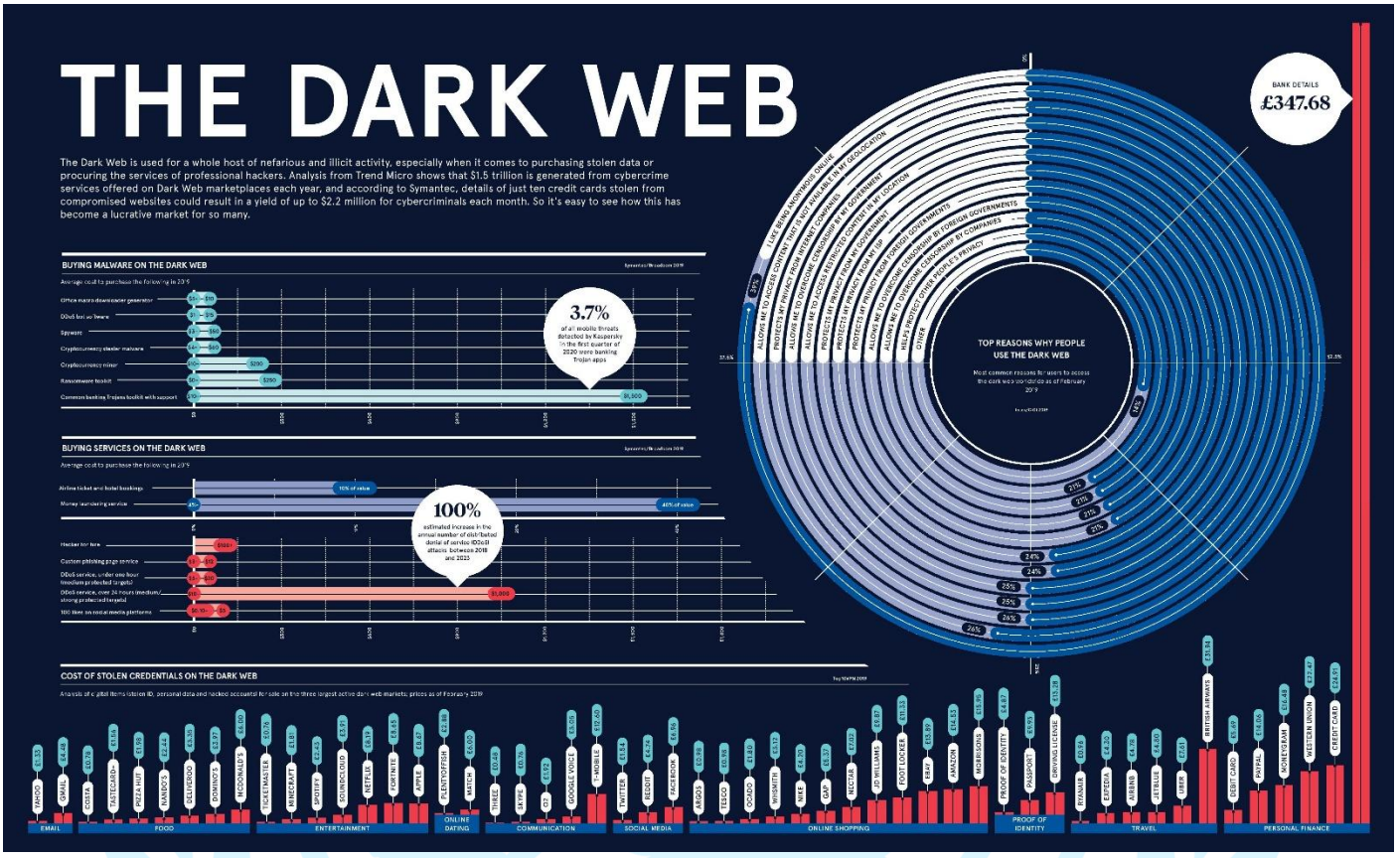
5. Strategic and Legal Foundations of Combating Dark Web Markets for Illicit Drugs and Arms

The anonymity provided by technologies like Tor and encryption tools makes it difficult for law enforcement to trace illegal activities, creating a complex legal landscape that transcends national borders. The lack of a unified international regulatory approach further complicates efforts to tackle cybercrime on the dark web. Additionally, the need to protect users' privacy while preventing criminal activities raises ethical concerns about the potential overreach of surveillance and the erosion of civil liberties.

It is important to analyse current regulatory attempts and underscore the importance of international cooperation, technological innovation, and clear legal frameworks to address the challenges effectively. It is also important to discuss the ethical implications of regulating the dark web, particularly the need to safeguard fundamental rights such as free speech and privacy.

The dark web's decentralized and global nature complicates the enforcement of territorial laws, as criminals can operate across borders, with servers hosted in jurisdictions that may lack robust cybercrime legislation. This borderless environment demands international cooperation, yet conflicting legal frameworks across countries exacerbate the problem. While some nations criminalize dark web usage for illicit purposes, others lack specific regulations or prioritize privacy over surveillance, creating safe havens for cybercriminals. For instance, the uneven adoption of the

Budapest Convention on Cybercrime reflects these disparities, with several major countries remaining outside its purview. Enforcement efforts are further hindered by technical barriers, such as encryption tools like Tor, resource gaps in developing nations, and coordination challenges among law enforcement agencies with differing priorities.



High-profile operations like the takedown of Silk Road and Europol's "Dark HunTor" demonstrate the necessity of cross-border collaboration but also reveal the logistical and ethical difficulties involved. Additionally, ethical concerns arise in balancing security with privacy, as surveillance technologies employed to track dark web activities risk infringing on civil liberties.

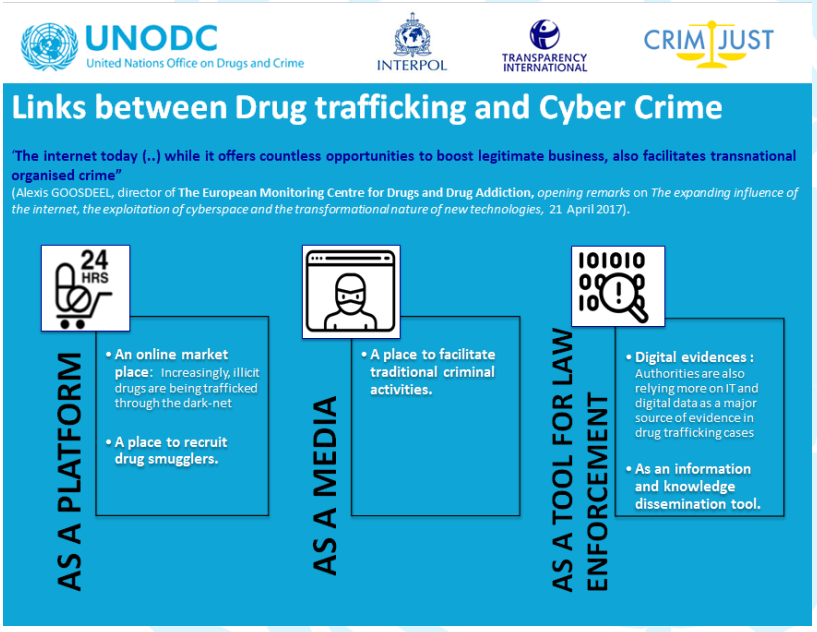
At the heart of dark web regulation lies the challenge of balancing privacy and security. The very technologies that protect anonymity, such as Tor (The Onion Router) and end-to-end encryption are also the same technologies that enable criminal activities. On the one hand, privacy protections are essential for users concerned about surveillance, oppression, or censorship. On the other hand, the same anonymity tools can provide cover for criminal networks. Striking the right balance between protecting individuals' right to privacy and enabling law enforcement agencies to investigate and prosecute illicit activities is crucial. Any regulation or intervention must consider the risks of overreach, which could lead to mass surveillance and infringements on fundamental rights.

Technology is both a boon and a barrier to effective regulation. The decentralized and encrypted nature of the dark web makes it difficult for law enforcement agencies to track criminal activities, such as drug trafficking or money laundering. While various technological tools and techniques, such as blockchain analysis or AI-powered surveillance, have been developed to detect and prevent illegal activities, the rapid evolution of technologies used by dark web users often outpaces regulatory efforts. For example, once one method of tracking dark web activity is implemented, new

tools or networks are quickly created to evade detection. The constant technological arms race between regulators and cybercriminals is one of the defining challenges in dark web governance.

a. Definition and Mechanisms of Dark Web Markets - anonymity tools (Tor, VPNs), cryptocurrency-based transactions, encrypted communications, escrow systems

Dark web markets are online platforms that operate within the hidden layers of the internet, beyond the reach of traditional search engines and standard browsers. These markets often facilitate the trade of illicit goods and services, though some legal products may also be found. What sets them apart is their reliance on advanced anonymity tools and secure mechanisms that make it difficult for authorities to track participants or shut down their operations. This environment has created a global ecosystem where individuals can engage in transactions while concealing their identities.



To maintain this anonymity, dark web markets commonly use tools such as Tor (The Onion Router) and VPNs (Virtual Private Networks). Tor directs traffic through multiple encrypted layers of servers, masking the user's IP address and location, while VPNs add an additional layer of protection by rerouting internet connections through secure networks. Alongside these tools, transactions are conducted primarily through cryptocurrencies like Bitcoin or Monero, which offer pseudonymous or enhanced privacy features. These mechanisms make it extremely difficult to trace payments back to real-world identities.

Communication and transactions on these markets are further safeguarded by encrypted messaging systems and escrow services. Encrypted communication ensures that buyers and sellers can only be understood by the intended parties, shielding conversations from interception. Escrow systems, meanwhile, act as intermediaries: funds are held securely until the buyer confirms delivery, reducing risks of fraud in an otherwise trustless environment. Together, these mechanisms form the backbone of dark web markets, combining anonymity, financial privacy, and security to sustain their operations.

b. Existing International Legal Frameworks - UN Convention against Transnational Organized Crime (UNTOC), UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), Firearms Protocol, and the role of UNODC's Cybercrime and Organized Crime Branch

The international community has established several legal frameworks to combat the threats posed

by organized crime, including those facilitated through cyberspace and dark web markets. Central to this is the UN Convention against Transnational Organized Crime (UNTOC), adopted in 2000, which serves as the primary global instrument for addressing organized criminal activity. UNTOC provides a comprehensive framework for states to criminalize participation in organized criminal groups, promote cooperation in investigations, strengthen extradition processes, and enhance mutual legal assistance. Its protocols extend its scope to specific areas, ensuring adaptability to evolving criminal trends.

Another key framework is the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which targets the global narcotics trade by criminalizing drug trafficking and strengthening international cooperation in countering drug-related offenses. Complementing this, the Firearms Protocol, adopted under UNTOC, focuses on preventing and combating the illicit manufacturing of and trafficking in firearms, their parts, and ammunition. Together, these instruments provide states with legal tools to address the trafficking of drugs, arms, and other illicit commodities often facilitated through online platforms, while ensuring international coordination and accountability.

Supporting the implementation of these frameworks is the United Nations Office on Drugs and Crime (UNODC), particularly through its Cybercrime and Organized Crime Branch. This branch plays a vital role in assisting Member States with legislative development, capacity-building, and technical assistance to tackle crimes that exploit technology, including those linked to organized criminal networks. By providing research, policy guidance, and training, UNODC ensures that states can effectively respond to the challenges posed by transnational crime in both physical and digital domains, reinforcing the international legal order.

c. Ethical and Human Rights Principles - balancing law enforcement with privacy rights, ensuring proportional surveillance, upholding due process, and avoiding overreach in digital governance

Addressing crime in the digital sphere requires a careful balance between effective law enforcement and the protection of individual privacy rights. While authorities must investigate and disrupt illicit activities such as those occurring on dark web markets, these efforts cannot come at the expense of fundamental freedoms. Upholding privacy is critical to maintaining public trust, as unchecked monitoring or invasive practices risk undermining democratic principles and individual liberties.

A key principle in this balance is the need for proportional surveillance. Governments and law enforcement agencies must ensure that investigative tools and monitoring mechanisms are targeted, justified, and limited to what is strictly necessary for the prevention or prosecution of crime. Broad or indiscriminate surveillance can lead to the erosion of civil liberties, disproportionately impacting innocent individuals while offering little added security. Proportionality ensures that the measures taken are effective without exceeding their legitimate purpose.

Equally important is the protection of due process and safeguards against overreach in digital governance. Individuals must retain their right to fair trials, access to justice, and protection from arbitrary or unlawful interference. Mechanisms of oversight, accountability, and transparency are essential to prevent abuse of power by state actors. By embedding ethical considerations and human

rights protections into digital governance frameworks, states can ensure that security and freedom reinforce rather than undermine one another.

6. Multilateral and Regional Frameworks for Tackling Dark Web-Enabled Illicit Trade

National Cybersecurity Laws: Many countries have enacted cybersecurity laws designed to combat online crime. However, these laws often struggle to keep up with technological advances. For example, the United States enforces the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA), while the European Union enforces protection laws. General Data Protection Regulation (GDPR) and Network and Information Systems Security Directive (SRI Directive). However, these regulations focus primarily on data protection and general cybersecurity. Instead, it is targeting the dark web. Moreover, the dark web's decentralized and boundaryless structure turns the law into an inadequate nationality in isolation. Cybercriminals often operate in jurisdictions with weak or non-existent cybercrime laws by exploring regulatory discrepancies this requires a more unified and international approach to law enforcement.

International Legal Cooperation: Computer crimes are considered transnational crimes. This requires international cooperation for effective mitigation. Organizations such as INTERPOL and the Council of Europe have initiated structures such as the Budapest Convention on Cybercrime. However, to harmonize such laws across countries, different legal systems political benefits and different levels of technological ability. This makes working together difficult. For example, countries such as Russia and China have not ratified the Budapest Convention. This limits global consensus on cracking down on cybercrime. The lack of universal oil infrastructure creates a haven for cybercriminals. Digging into global efforts to combat dark web activity.

Challenges in Law Enforcement: Law enforcement agencies face significant obstacles in investigating the dark web. The anonymity provided by encryptions such as Tor and the use of cryptocurrencies for transactions makes it difficult to track down and prosecute perpetrators. Additionally, the emergence of decentralized markets and peer-to-peer networks. Peer-to-peer complicates surveillance and infiltration. High-profile hacks such as the Silk Road and Alpha Bay arrests demonstrate that law enforcement can disrupt Dark Web operations. However, these victories are often short-lived. Because new markets happen quickly the flexibility of the dark web underscores the inadequacy of traditional legal and police methods.

a. UN-Based Mechanisms - UNODC's Global Programme on Cybercrime, the Commission on Narcotic Drugs (CND), the Firearms Working Group, and the Conference of the Parties to UNTOC

The United Nations has established several mechanisms to address the intersection of organized crime, cybercrime, and illicit trade, with the UNODC's Global Programme on Cybercrime serving as a central pillar. This programme provides technical assistance, training, and legislative guidance to Member States to enhance their ability to investigate and prosecute cybercrime. It also fosters international cooperation by connecting national authorities and promoting best practices in digital

forensics, online investigations, and strategies to combat illicit use of the dark web, ensuring that states with varying levels of capacity can respond effectively.

Complementing this, the Commission on Narcotic Drugs (CND) acts as the principal policymaking body within the UN system for drug-related matters. It monitors global trends in narcotic drugs and psychotropic substances, sets international drug control standards, and guides Member States in implementing the 1988 UN Drug Convention. With the growing use of online platforms and darknet markets for drug trafficking, the CND increasingly considers the technological dimension of the drug trade, encouraging states to address both traditional and digital channels of illicit distribution.

Other specialized mechanisms further strengthen this system. The Firearms Working Group supports the implementation of the Firearms Protocol by assisting states in preventing, detecting, and addressing illicit arms trafficking, including cases facilitated through online channels. Meanwhile, the Conference of the Parties to UNTOC (COP-UNTOC) ensures the effective review and implementation of the UNTOC and its protocols, providing a forum for states to assess progress, share challenges, and develop new strategies against transnational organized crime. Collectively, these UN-based mechanisms form a comprehensive network that addresses crime across multiple domains, including its increasingly digital dimensions.

b. Regional Approaches - Europol's European Cybercrime Centre (EC3), African Union's regional anti-narcotics strategies, Organization of American States' Inter-American Drug Abuse Control Commission (CICAD), and Asia-Pacific Economic Cooperation (APEC) cybersecurity dialogues

Regional organizations have developed targeted strategies to counter the rise of dark web–enabled illicit trade, recognizing that localized cooperation can complement global frameworks. In Europe, Europol's European Cybercrime Centre (EC3) plays a leading role in combating online crime, including drug trafficking, cyber fraud, and illicit markets hosted on the dark web. EC3 facilitates intelligence-sharing, joint operations, and advanced forensic support, enabling EU member states to coordinate cross-border investigations and dismantle organized crime groups operating in digital environments.

In Africa, the African Union (AU) has prioritized combating narcotics trafficking through regional strategies that also account for the digital dimension of drug markets. These strategies emphasize capacity-building for law enforcement, judicial cooperation, and the establishment of early-warning systems to track and disrupt drug flows. By promoting coordination between national agencies and regional bodies, the AU seeks to strengthen the resilience of its member states against both traditional trafficking routes and newer, technology-driven channels that exploit the dark web.

Across the Americas and the Asia-Pacific, regional initiatives also address the nexus between cybercrime and illicit trade. The Organization of American States (OAS), through its Inter-American Drug Abuse Control Commission (CICAD), develops policy guidelines, research, and training to support member states in tackling drug trafficking, including cases where darknet platforms are used. Meanwhile, the **Asia-Pacific Economic Cooperation (APEC) engages in cybersecurity dialogues that bring together policymakers, experts, and private sector actors to strengthen digital governance and protect economic systems from online threats. Together, these regional approaches highlight the importance of tailoring responses to local contexts while fostering cooperation across borders to

counter dark web–enabled criminal networks.

c. Other Stakeholders - INTERPOL, Financial Action Task Force (FATF), World Customs Organization (WCO), private cybersecurity firms, blockchain analytics companies, and research institutions working on dark web monitoring.

Alongside UN and regional mechanisms, several international and independent stakeholders play an important role in combating dark web–enabled illicit trade. INTERPOL provides a global platform for police cooperation, supporting cross-border investigations and real-time information exchange on cybercrime and illicit trafficking. Its cybercrime directorate assists national law enforcement agencies with capacity-building and coordinated operations against online criminal networks. Similarly, the Financial Action Task Force (FATF) sets global standards for anti–money laundering and counter-terrorism financing, which are critical for disrupting the cryptocurrency-based transactions that underpin many dark web markets.

Specialized organizations like the World Customs Organization (WCO) also contribute by focusing on illicit trade that crosses borders physically after being facilitated online. The WCO develops risk management strategies, promotes data exchange among customs agencies, and helps detect shipments linked to dark web purchases, such as drugs, firearms, or counterfeit goods. These measures close the gap between online activity and its offline consequences, ensuring that illicit goods are intercepted before reaching consumers.

Beyond intergovernmental bodies, the private sector and academia provide crucial expertise. Private cybersecurity firms and blockchain analytics companies track illicit transactions, trace cryptocurrency flows, and monitor dark web marketplaces to provide actionable intelligence to law enforcement. Meanwhile, research institutions conduct in-depth studies on dark web ecosystems, criminal methodologies, and emerging trends, offering insights that shape public policy and enforcement strategies. The collaboration of these diverse stakeholders creates a multi-layered response, combining law enforcement, regulatory oversight, technological innovation, and academic research to address the evolving challenges of the dark web.

7. Political and Security Challenges in Governing Dark Web Markets

The emergence of dark web marketplaces has created one of the most pressing governance challenges of the digital age. These platforms, which rely entirely on advanced anonymity technologies and decentralized financial systems, enable the global trade of illicit narcotics, firearms, counterfeit documents, and other prohibited goods. Unlike traditional forms of organized crime, dark web markets exist within a borderless and encrypted digital ecosystem, resistant to conventional law enforcement tools and operating beyond the reach of single jurisdictions. This reality has transformed what were once localized black-market dynamics into highly globalized supply chains, enabling criminal actors to operate with resilience, flexibility, and impunity.

These challenges may be broadly understood through three interrelated dimensions: interconnected domains: the risks created by cryptocurrencies and anonymity tools, the difficulties of attribution and jurisdictional enforcement, and the increasingly prominent role of non-state actors who exploit

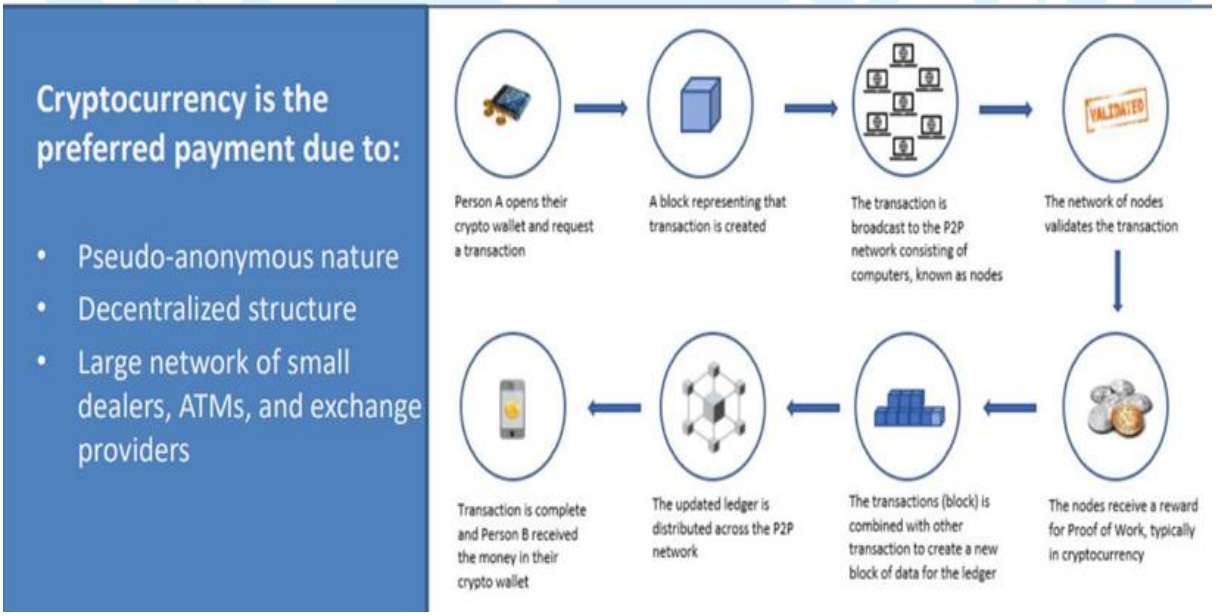
these platforms to advance their objectives.

a. Risks of Cryptocurrencies and Anonymity Tools - laundering illicit profits, evading financial monitoring systems.

One of the defining features of dark web markets is the reliance on cryptocurrencies and anonymity-enhancing technologies that enable illicit activities to flourish beyond the reach of conventional financial monitoring and law enforcement mechanisms. These tools are not inherently criminal; indeed, they serve legitimate purposes such as privacy protection, digital security, and financial inclusion. However, when exploited by organized crime groups, terrorist networks, and arms traffickers, they become powerful enablers of transnational criminal economies.

Cryptocurrencies such as Bitcoin, Monero, and Ethereum play a central role in dark web marketplaces, serving as the preferred medium of exchange for illicit drugs, firearms, counterfeit goods, and other prohibited commodities. Unlike traditional financial systems that rely on centralized intermediaries such as banks, cryptocurrencies operate on decentralized blockchain networks, reducing the ability of regulatory bodies to monitor and intercept suspicious transactions.

Bitcoin initially dominated the dark web due to its accessibility and widespread adoption. However, as law enforcement agencies and blockchain analytics firms developed the ability to trace Bitcoin transactions, cybercriminals increasingly migrated toward privacy-oriented such as Monero and Zcash. These currencies employ advanced obfuscation techniques such as ring signatures, stealth addresses, and zero-knowledge proofs, making it significantly harder to trace transaction flows. This shift reflects the adaptability of criminal actors and the constant technological arms race between regulators and illicit networks.



The Silk Road marketplace (2011-2013), one of the earliest and most infamous examples of dark web trade, exclusively used Bitcoin for transactions, which ultimately contributed to its takedown when investigators traced wallet addresses linked to Ross Ulbricht. By contrast, in later cases such as AlphaBay (2017), administrators encouraged the use of Monero precisely because it was

designed to resist blockchain tracking. This evolution highlights how cryptocurrency risks are not static but evolve alongside law enforcement strategies.

Cryptocurrencies also facilitate the laundering of illicit profits. Through mechanisms such as "mixing" or "tumbling" services, criminals can blend their digital funds with legitimate transactions, obscuring the original source. These services, along with Decentralized Exchanges (DEXs), allow illicit actors to rapidly convert between currencies and jurisdictions, bypassing traditional Anti-Money Laundering (AML) safeguards. The Financial Action Task Force (FATF) has attempted to impose global standards on cryptocurrency service providers through the so-called "travel rule," requiring exchanges to record and share information about transaction originators and beneficiaries.

However, enforcement remains uneven, with significant gaps in jurisdictions where regulatory frameworks are weak or non-existent. Alongside cryptocurrencies, anonymity tools such as Tor (The Onion Router) and virtual private networks (VPNs) are indispensable to the functioning of dark web markets. Tor routes internet traffic through multiple relays across the globe, encrypting it at every step and effectively concealing the user's identity and location. This prevents conventional law enforcement monitoring and makes attribution of criminal activity exceedingly difficult. VPNs serve a similar function by masking a user's IP address and encrypting communications, further complicating digital investigations.

These technologies are often combined with encrypted messaging services such as Signal or Telegram, which allow vendors and buyers to coordinate transactions beyond the visibility of conventional monitoring systems. The widespread availability of these tools means that even individuals with limited technical knowledge can engage in sophisticated anonymized transactions.

However, their use is not confined to criminal activity. Tor, VPNs, and encryption are vital for journalists, political dissidents, and human rights defenders operating under repressive regimes. This dual-use nature creates a political dilemma: excessive regulation or surveillance of these tools may undermine civil liberties and digital rights, while insufficient oversight leaves them open to criminal misuse. For example, China and Russia have sought to restrict access to Tor and VPNs, framing their actions as crime prevention measures, while critics argue these policies also suppress political dissent.

The proliferation of anonymity tools and cryptocurrencies significantly complicates the political and security landscape. By enabling terrorists, drug cartels, and arms traffickers to conduct transactions with reduced risk of detection, they undermine state capacity to enforce law and order. The use of cryptocurrencies by non-state actors, including groups linked to terrorism financing such as ISIS, has raised global alarm. In 2020, the U.S. Department of Justice dismantled a network of websites used by ISIS, Al-Qaeda, and Hamas to solicit donations in Bitcoin and other cryptocurrencies, underscoring the nexus between cyber tools and international security threats.

Moreover, state and non-state actors alike may exploit these tools for geopolitical advantage. There have been allegations of North Korea's involvement in cryptocurrency thefts and laundering schemes, using the proceeds to finance weapons development programs despite international sanctions. Such examples demonstrate that the risks are not limited to criminal syndicates but also extend to broader questions of international peace and security.

b. Challenges in Attribution, Jurisdiction, and Law Enforcement Coordination - identifying perpetrators across borders, conflicting national laws, evidence admissibility.

One of the most complex aspects of governing dark web markets lies in the ability of states to identify perpetrators, establish jurisdiction, and coordinate law enforcement across multiple borders. Unlike conventional crimes where suspects and evidence are often contained within a single territorial jurisdiction, cyber-enabled crimes thrive in a transnational environment. Dark web marketplaces often operate on anonymized servers, use encryption to conceal identities, and rely on decentralized payment systems, making attribution and enforcement exceedingly difficult.

'Attribution' refers to the process of identifying the individuals or groups responsible for criminal activity on the dark web. This process is complicated by the use of anonymity tools such as Tor networks, Virtual Private Networks (VPNs), and proxy servers, which mask the digital footprints of users. For example, the administrator of the infamous Silk Road marketplace, Ross Ulbricht, was only identified after months of complex digital tracing combined with offline investigative work. In many other cases, anonymity tools succeed in concealing identities long enough for marketplaces to disappear or rebrand, making law enforcement efforts ineffective. Moreover, the use of false identities, layered accounts, and sophisticated obfuscation techniques creates scenarios where attribution errors risk accusing innocent individuals, undermining the credibility of enforcement agencies.

Jurisdictional challenges arise because dark web crimes usually involve multiple states simultaneously. A single illicit arms transaction might involve a vendor based in Eastern Europe, servers hosted in Southeast Asia, a cryptocurrency wallet located on an exchange in Latin America, and a buyer based in North America. Each of these states may claim jurisdiction over part of the activity, yet conflicting national laws often prevent coherent legal action. For instance, while some countries classify cryptocurrency transactions as traceable financial activities subject to AML regulations, others either lack relevant legislation or permit them as legitimate financial exchanges, creating "safe havens" for cybercriminals.

The issue of *evidence* admissibility compounds these challenges. Digital evidence collected in one jurisdiction may not meet the legal standards of another. For example, metadata gathered without a court order in one state may be deemed inadmissible in another with stricter due process requirements. Similarly, surveillance techniques such as packet sniffing, deep packet inspection, or infiltration of online communities may be legally permissible in some jurisdictions but considered violations of privacy rights elsewhere. Such discrepancies create loopholes that defense attorneys can exploit, leading to acquittals despite strong evidence of wrongdoing.

Law enforcement coordination is further undermined by bureaucratic and political obstacles. While Mutual Legal Assistance Treaties (MLATs) were designed to facilitate cooperation, they are often too slow to address the rapidly evolving nature of dark web marketplaces. By the time evidence requests are processed, servers may have been relocated, accounts deleted, or cryptocurrencies laundered through mixers and tumblers, erasing the trail. Efforts like the Joint Criminal Opioid and Darknet Enforcement (J-CODE) team in the United States or Europol's European Cybercrime Centre (EC3) have achieved notable successes, such as the takedown of AlphaBay and Hansa Market in 2017. However, these examples highlight that success often depends on highly specialized capacities and close trust between a limited number of advanced states, leaving many countries excluded from meaningful participation.

The lack of uniformity in legal frameworks and investigative capacity results in uneven enforcement. Criminal actors exploit these gaps by deliberately situating their operations in jurisdictions with weak laws, minimal oversight, or reluctance to cooperate internationally. This "jurisdictional arbitrage" ensures that even if one country cracks down, operations can quickly relocate to another, sustaining the resilience of dark web markets.

Ultimately, the challenge of attribution, jurisdiction, and coordination underscores the need for harmonized legal frameworks, faster mechanisms for cross-border evidence exchange, and greater capacity-building for developing countries. Without addressing these systemic weaknesses, the dark web will continue to provide a relatively safe haven for traffickers of drugs and arms.

c. Threat of Non-State Actors - terrorist groups, cartels, and arms traffickers exploiting the dark web to acquire funding and weaponry.

The exploitation of dark web markets by non-state actors represents a critical dimension of the political and security challenges associated with illicit online trade. These actors, which include terrorist organizations, transnational criminal cartels, and arms traffickers, leverage the unique capabilities of the dark web to advance both financial and operational objectives while avoiding detection by traditional law enforcement. Unlike conventional criminal enterprises, these actors operate across borders, often coordinating complex networks that integrate drug trafficking, arms sales, money laundering, and cybercrime, thereby amplifying their impact on global security.

Terrorist organizations have increasingly turned to dark web marketplaces as a means of raising funds. Cryptocurrencies allow these groups to solicit donations from global sympathizers while evading conventional banking systems and financial regulations. Europol and UNODC reports indicate that ISIS-affiliated entities and other extremist groups have maintained digital presences on encrypted forums, soliciting contributions and even exchanging operational instructions. The anonymity provided by Tor and other hidden networks ensures that communications, recruitment,

and fundraising activities remain largely insulated from law enforcement scrutiny, creating persistent challenges for counter-terrorism initiatives.

Transnational criminal cartels have also integrated dark web markets into their operational frameworks. Platforms such as Hydra, AlphaBay, and Silk Road facilitated the global distribution of illicit drugs, counterfeit documents, and other contraband while concealing the identities of vendors and buyers. These marketplaces not only expand the geographical reach of cartels but also enhance their ability to coordinate logistics and evade local law enforcement. Hydra, for instance, served millions of users worldwide and was linked to large Russian-speaking organized crime networks, demonstrating the capacity of dark web markets to function as hubs for complex transnational operations.

The dark web also enables arms traffickers to circumvent national and international regulations governing the sale of firearms and explosives.

> The 2016 Munich shooting exemplifies the dangers posed by the online arms trade, as the perpetrator acquired a Glock pistol via a darknet vendor, bypassing Germany's strict legal restrictions. Europol has consistently highlighted the growth of weapons sales on encrypted platforms, noting that even limited transactions can have severe consequences when firearms reach individuals or groups outside legal channels.

The convergence of these non-state actors on the dark web generates systemic risks. It facilitates the intersection of terrorism, organized crime, and illicit arms distribution, creating a self-reinforcing ecosystem in which criminal innovation outpaces law enforcement capabilities. The transnational and encrypted nature of these activities complicates traditional investigative approaches and necessitates a coordinated international response. This requires the active involvement of multilateral institutions such as UNODC, INTERPOL, and regional enforcement mechanisms to monitor, analyze, and disrupt illicit networks while simultaneously addressing the technological, legal, and operational gaps that allow non-state actors to exploit dark web marketplaces.

8. Geopolitical Complexities and Strategic Ambiguities in Addressing Dark Web Crimes

The dismantling of dark web markets for illicit drugs and arms does not occur in a vacuum of law enforcement; it is inextricably tied to geopolitics and the strategic behavior of states. Unlike traditional organized crime, the dark web operates in a borderless digital space, complicating the application of national laws and creating tension between sovereignty, security, and international cooperation. States approach the problem through divergent strategies, often shaped by their political priorities, technological capacity, and perceptions of digital governance. This uneven landscape generates ambiguities that transnational criminal groups exploit to sustain and expand their operations.

a. Divergent National Approaches - varying national cybercrime laws, differences in regulating cryptocurrencies, and capacity gaps in digital forensics.

Addressing dark web markets for illicit drugs and arms is complicated by stark divergences in national approaches to cybercrime governance. Unlike traditional transnational criminal activities, which are governed through relatively well-established treaties, cyber-enabled crimes reveal persistent gaps in global governance, fragmented legal frameworks, and unequal technological capacities among states.

The absence of a universally binding legal regime for cybercrime is a major barrier to international cooperation. The Budapest Convention on Cybercrime of 2001, spearheaded by the Council of Europe, remains the only binding multilateral treaty in this domain. While the European Union, the United States, and over 60 other states have acceded to it, key global powers including Russia, China, and India have declined participation. Their objections stem largely from concerns over sovereignty and the dominance of Western states in shaping cyber norms. As a result, darknet operators often exploit jurisdictions outside Budapest's framework, establishing safe havens where enforcement is weak or non-existent.

For example, Russian authorities have historically been reluctant to prosecute cybercriminals operating from their territory as long as their activities targeted foreign entities. This policy of non-extradition and selective enforcement has been a recurring friction point between Russia and Western states, particularly the United States, which has sought the extradition of high-profile cybercriminals. Such gaps directly undermine the creation of a coherent global enforcement architecture.

Cryptocurrencies, especially Bitcoin and privacy-focused alternatives such as Monero, form the financial backbone of dark web transactions. States vary drastically in how they regulate these currencies. Japan requires cryptocurrency exchanges to comply with stringent Anti-Money Laundering and Counter-Terrorism Financing regulations under its Financial Services Agency. Exchanges must conduct Know Your Customer verification and report suspicious activities. In contrast, El Salvador's 2021 decision to adopt Bitcoin as legal tender provides users with significant transactional anonymity, inadvertently creating opportunities for illicit actors to exploit its system for laundering proceeds from darknet sales. Meanwhile, China has banned cryptocurrency trading and mining entirely, citing concerns about financial instability and illicit use. However, this has primarily driven underground networks rather than eliminating crypto-enabled crime.

The Financial Action Task Force has attempted to harmonize global standards through its "Travel Rule," which requires Virtual Asset Service Providers to share sender and recipient information in crypto transactions. Yet implementation remains uneven, with non-compliant jurisdictions offering safe zones for laundering darknet proceeds.

Another critical dimension of divergence lies in technological and institutional capacity. Advanced economies such as the United States, the United Kingdom, Germany, and the Netherlands possess highly specialized cybercrime units capable of blockchain analytics, darknet infiltration, and cyber-forensic reconstruction. Their capabilities have enabled landmark takedowns such as Silk Road in 2013, which was dismantled by the U.S. Federal Bureau of Investigation through Bitcoin transaction tracing and the arrest of its founder Ross Ulbricht. Similarly, the joint Europol-FBI operation in 2017 led to the takedown of AlphaBay and Hansa Market. Law enforcement secretly seized control of

Hansa Market before shutting down AlphaBay, effectively trapping users and harvesting intelligence for ongoing investigations.

In stark contrast, many developing nations in Africa, Asia, and Latin America lack even basic cyber-forensic infrastructure. For instance, INTERPOL's 2021 African Cyberthreat Assessment Report noted that several member states lacked functioning cybercrime units, leaving them unable to investigate darknet-enabled drug trafficking despite being transit hubs for narcotics. These states are thus disproportionately reliant on intelligence from technologically advanced powers, reinforcing perceptions of dependency and asymmetry.

This divergence produces a patchwork of enforcement standards that darknet operators exploit through regulatory arbitrage. Criminal groups establish operational bases in jurisdictions with weak enforcement but target consumers globally, often moving their operations once a crackdown occurs. The cycle of takedown and migration, observed in successive closures of Silk Road, AlphaBay, and Wall Street Market, demonstrates how uneven national approaches prevent the establishment of a sustainable enforcement regime.

Ultimately, while some states are equipped and willing to aggressively pursue darknet markets, others lack the legal frameworks, political will, or technical capacity to engage. This fragmented landscape continues to be a core obstacle in dismantling dark web markets for illicit drugs and arms, highlighting the urgent need for harmonization, capacity building, and equitable participation in global cyber governance.

b. Jurisdictional Overlaps and Sovereignty Concerns - cross-border data requests, mutual legal assistance treaties (MLATs), and tensions between intelligence sharing and state secrecy.

Dark web markets for illicit drugs and arms operate across multiple jurisdictions simultaneously, making enforcement highly complex. A single marketplace may rely on servers hosted in one country, administrators in another, and customers spread across dozens of states. This transnational nature of darknet crime exposes legal overlaps, conflicting claims of jurisdiction, and recurring sovereignty disputes.

Investigations into dark web crimes often depend on evidence stored in foreign jurisdictions, such as server logs, communication records, or blockchain transaction data. The primary legal mechanism for such cooperation is the Mutual Legal Assistance Treaty (MLAT) framework. While MLATs provide a recognized process for states to exchange data, they are often criticized for being slow and bureaucratically cumbersome. In practice, requests can take months or even years, while darknet platforms typically operate on much shorter life cycles.

This mismatch between investigative timelines and procedural delays has undermined many international investigations. For example, European cybercrime units have frequently cited delays in obtaining data from U.S.-based service providers, while U.S. authorities have raised similar complaints about jurisdictions where data protection rules or judicial bottlenecks slow cooperation. Such inefficiencies leave enforcement efforts trailing behind fast-evolving darknet networks.

Beyond formal legal channels, international operations often rely on intelligence sharing between

agencies. However, such cooperation is constrained by national security concerns and the protection of sensitive investigative methods. States are frequently reluctant to disclose details about advanced cyber-forensic tools, blockchain-tracing software, or infiltration techniques. This reluctance preserves national advantage but reduces opportunities for building collective capacity.

A recurring concern is the dual-use nature of cyber capabilities. Tools developed for countering darknet markets can also serve broader geopolitical objectives such as surveillance or espionage. This fuels mistrust among states, particularly between advanced and developing economies, as well as between geopolitical rivals. As a result, intelligence sharing remains selective and uneven, with major powers often accused of monopolizing technological advantages.

Sovereignty concerns are most acute when law enforcement agencies act unilaterally across borders. Operations that involve remotely accessing servers or data located in foreign jurisdictions without explicit approval raise accusations of interference and legal overreach. These disputes are especially visible in the context of strained relations between Western states and countries such as Russia or China.

For instance, Russia has consistently refused to extradite its nationals accused of cybercrimes abroad, asserting that they should be prosecuted domestically. At the same time, Western agencies argue that crimes targeting their citizens or infrastructure fall under their jurisdiction, creating persistent diplomatic clashes. Similarly, Chinese officials have objected to foreign cyber operations that penetrate infrastructure hosted on their territory, framing such actions as violations of sovereignty.

The lack of clear jurisdictional boundaries and the persistence of sovereignty disputes leave significant blind spots in global enforcement. Darknet operators exploit these gaps by distributing their infrastructure across multiple jurisdictions, complicating investigations and delaying enforcement. Without reforms that streamline cross-border data requests, build mutual trust in intelligence cooperation, and establish clearer norms on jurisdiction in cyberspace, enforcement against darknet markets will remain fragmented and reactive.

c. Perceptions of Technological Asymmetry - advanced digital policing capabilities concentrated in developed states, leaving developing states vulnerable to exploitation and widening enforcement gaps.

The enforcement of dark web crimes is deeply shaped by global inequalities in technological capacity. While advanced economies have invested heavily in cybercrime units, blockchain analytics, and digital forensics, many developing states lack even the most basic infrastructure to counter darknet activities. This imbalance creates not only operational vulnerabilities but also political perceptions of dependency and exclusion, which in turn complicate international cooperation.

Agencies in the western countries possess highly specialized digital policing tools and dedicated institutions. The European Cybercrime Centre (EC3) at Europol and the Federal Bureau of Investigation (FBI) in the United States have pioneered the use of blockchain tracing, undercover infiltration of darknet forums, and artificial intelligence-based monitoring systems. Their coordinated actions have resulted in significant successes, including the dismantling of large-scale

marketplaces such as Wall Street Market and Dream Market. These operations highlight the effectiveness of advanced cyber-forensic methods when backed by sufficient resources and expertise.

In contrast, many developing states face structural barriers, including a shortage of trained cyber investigators, lack of forensic laboratories, and inadequate legal frameworks to authorize digital surveillance. According to INTERPOL's 2021 African Cyberthreat Assessment, several countries on the continent lack national cybercrime units altogether, despite being used as logistical or financial transit hubs for darknet-enabled narcotics trafficking. This disparity leaves developing states particularly vulnerable to exploitation by transnational criminal groups.

The uneven distribution of capabilities contributes to widening enforcement gaps. Criminal actors deliberately route their operations through jurisdictions with limited technical oversight, exploiting weak monitoring systems and scarce forensic capacity. For example, darknet administrators often rely on bulletproof hosting services in states with limited enforcement capabilities, making it extremely difficult for foreign agencies to secure timely cooperation.

This asymmetry also reinforces a cycle of dependency. Developing countries frequently rely on intelligence and technical assistance from advanced powers to pursue investigations, as seen in Latin American states requesting digital forensics support from U.S. agencies during narcotics-related cyber investigations. While such support strengthens short-term enforcement, it also deepens perceptions of inequality and questions of sovereignty, as developing states fear becoming permanently reliant on external actors for cyber governance.

Beyond operational challenges, technological asymmetry generates broader geopolitical tensions. Advanced powers are often perceived as monopolizing cutting-edge surveillance and investigative technologies, while selectively sharing them based on political or strategic considerations. This perception undermines trust in multilateral forums, as states question whether digital policing capabilities are being deployed for collective security or leveraged for geopolitical advantage.

For example, debates in United Nations forums have revealed *skepticism* from developing countries, which argue that cybercrime enforcement frameworks disproportionately reflect Western technological standards. Similarly, concerns over unequal access to forensic tools, such as blockchain analytics software controlled by Western private firms, which fuel suspicions that enforcement power is concentrated in the hands of a few actors.

Perceptions of technological asymmetry thus carry both practical and political consequences. Practically, enforcement gaps allow darknet markets to exploit weak jurisdictions with relative impunity. Politically, the perception of unequal access to cyber capabilities erodes trust and hinders consensus on shared frameworks for dismantling illicit markets. Unless international cooperation prioritizes capacity building, technology transfer, and equitable participation, the fight against dark web crime will remain skewed toward developed states, leaving vulnerable regions exposed to exploitation.

9. Questions a Resolution Should Address

- How should “dark web markets” be formally defined to include anonymity technologies (Tor, VPNs), cryptocurrencies, escrow systems, and encrypted communications within an international legal context?
- Should member states work toward a harmonized legal definition of “dark web crimes” to ensure consistency in extradition, prosecution, and sentencing? (Basic necessity for a legally definition)
- What jurisdictional challenges arise when servers, perpetrators, and victims are located in different states?
- How can existing UN legal instruments such as the UNTOC, Firearms Protocol, and the 1988 Vienna Convention on Drugs be expanded to explicitly cover crimes conducted via encrypted and anonymized platforms like the dark web?
- How can intelligence-sharing frameworks (e.g., INTERPOL I-24/7, Europol EC3) be strengthened to allow secure, real-time exchange of cyber forensic data and operational alerts?
- What advanced methodologies can be employed to trace cryptocurrency transactions (mixers, tumblers, privacy coins) linked to illicit drug and arms sales on the dark web?
- What forensic technologies (scraping mechanisms, blockchain forensics, machine learning for pattern recognition) can be deployed to detect, monitor, and dismantle illicit markets on the dark web?
- What frameworks can mitigate the perception of “technological asymmetry,” where advanced cyber capabilities are concentrated in a few states while developing states lack adequate capacity?
- How can Mutual Legal Assistance Treaties (MLATs) and cross-border data-sharing agreements be modernized to account for encrypted communications, anonymized routing systems, and decentralized hosting infrastructures?
- To what extent can global attribution mechanisms be developed to identify and hold accountable perpetrators of dark web crimes, despite obfuscation through spoofing, layered proxies, and anonymizing tools?
- How should states address the dual-use dilemma, where privacy-enhancing technologies (end-to-end encryption, Tor routing) are simultaneously essential for human rights defenders and journalists but also exploited by criminals on the dark web?
- What regulatory approaches can be developed to hold cryptocurrency exchanges, peer-to-peer platforms, and decentralized finance (DeFi) networks accountable for facilitating transactions linked to illicit markets?
- How can the committee ensure that responses to dark web crimes do not undermine fundamental principles of state sovereignty, digital rights, and international humanitarian law?
- What monitoring and verification mechanisms can be introduced to assess compliance by states and private entities in implementing counter-dark web crime measures?
- How can international law enforcement operations (e.g., Operation Onymous, Operation Bayonet) serve as precedents in assessing both the feasibility and limitations of dismantling large-scale dark web markets?

10. Important Links

- UNAUSA Rules of Procedure
  drive.google.com/file/d/1Up_8hAqWkjBM1CDmfb5DgNj9908f0VJJ/view
- UN Charter
  https://treaties.un.org/doc/publication/ctc/uncharter.pdf
- Malcolm Shaw - International Law
  https://drive.google.com/file/d/1Ap59YQ1dbtpCVoQtJGIswl-FkAWPz0Cu/view
- United Nations Office of Drugs and Crimes (UNODC)
  https://www.unodc.org/
- The Commission on Crime Prevention and Criminal Justice
  https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html
- Commission on Narcotics and Drugs (CND)|
  https://www.unodc.org/unodc/en/commissions/CND/index.html
- UN Commission on Narcotic Drugs (CND) Resolution 65/2
  www.unodc.org/documents/commissions/CND/Drug_Resolutions/2020-2029/2022/Res_65_2.pdf
- Transnational Organized Crime and the Convergence of Illicit Markets (A 2024 regional study by the UNODC Southeast Asia and the Pacific office exploring how cybercriminal ecosystems, including darknet marketplaces)
  https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
- In Focus: Trafficking over the Darknet (2020 World Drug Report)
  https://www.unodc.org/documents/Focus/WDR20_Booklet_4_Darknet_web.pdf
- EUROPOL Internet Organised Crime Threat Assessment (IOCTA) 2024
  https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
- AlphaBay: How Seven Countries Worked Together to Take Down the Biggest Online Black Market for Drugs
  https://www.unodc.org/unodc/untoc20/truecrimestories/alphabay.html
- UNODC World Report 2024
  www.icati.org/knowledge-share/resources/2024-07/unodc-world-drug-report-2024
- Use of the Dark Web and Social Media for Illicit Markets (UNODC)
  https://www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf
- UNODC-Tools and Programs to Address Illicit Online Drug Sales on the Open and Dark Web
  https://www.state.gov/wp-content/uploads/2021/11/UNODC-Tools-and-Programs-to-Address-Illicit-Online-Drug-Sales-on-the-Open-and-Dark-Web.pdf
- CRIMJUST & Global Cybercrime Programme explored the use of web associated tools by organized criminal networks for the purpose of illicit drug trafficking.
  https://www.unodc.org/unodc/en/drug-trafficking/crimjust/news/crimjust-and-global-cybercrime-programme-explored-the-use-of-web-associated-tools-by-organized-criminal-networks-for-the-purpose-of-illicit-drug-trafficking.html
- Marketness and Governance: A Typology of Illicit Online Markets
  www.tandfonline.com/doi/full/10.1080/01639625.2024.2323526

- UNODA Occasional Paper No.32: “The Trade in Small Arms and Light Weapons on the Dark Web: A Study” https://drive.google.com/file/d/1RkEzcAY7drzZ_VMaS79PnDFTY11bqBU6/view?usp=sharing
- Assessing the Practices and Products of Darkweb Firearm Vendors https://drive.google.com/file/d/1WDkPKJS9OBSqCxms2n4YrAYsDGLHprrC/view?usp=sharing