**Blue Bells Model United NATIONS**

**CONFERENCE**



**Blue Bells for World Peace**

**UNITED NATIONS OFFICE ON DRUGS AND CRIME**

**BACKGROUND GUIDE**

**AGENDA : Discussing the laws of cyber crime with emphasis on online drug trafficking**

**Letter from the Executive Board**

Dear Delegates,

It is an honor to be serving as the Executive Board of the United Nations Office of Drugs and Crime at The Blue Bells MUN Conference’19.

Please consider that the aim of this guide, as the name suggests, is to provide you with the background of the agenda solely. Your real research lies beyond this guide and we hope to see strong content and debate in the conference.

The topic under discussion is, “Discussing the laws of cybercrime with emphasis on online drug trafficking”.

The agenda at hand is a highly sensitive and relevant issue, and a successful discussion on it would entail the collective participation of all of you. As far as the direction of the committee is concerned, it shall be entirely your prerogative.

Also apart from simple knowledge of facts and figures that you gain while researching, analysing and connecting to the same on a more intellectual and emotional level is necessary while approaching a situation like this.

Lastly, put your best foot forward as you research into the varied aspects of the agenda and display the best of your diplomatic courtesy. Feel free to revert back to the executive board for any queries or for any form of assistance that you may require. Wishing you luck for the conference.

**Note – It is mandatory for all delegates to go through the questions to consider and provided at the end of the background guide.**

Looking forward to meet you all!

Yash Gupta

Advaya Shukla

(advayashukla@gmail.com)

**About the Committee**

The then-Office for Drug Control and Crime Prevention was set up in 1997, merging the UN Drug Control Programme and the Centre for International Crime Prevention. In 2002 the organization was renamed the UN Office on Drugs and Crime (UNODC). The UNODC operates via field offices in various states, and 90% of its budget is dependent on voluntary state contributions. The UNODC’s mandate is to ‘assist Member States in their struggle against illicit drugs, crime and terrorism’ – a fairly wide remit.

The organisation reflects today’s modern recognition of the interconnectivity between crime, drugs, terrorism and the international dimension. Its work also operates on ‘three pillars’:

• Field-based technical cooperation projects to enhance the capacity of Member States to counteract illicit drugs, crime and terrorism’

• Research and analytical work to increase knowledge and understanding of drugs and crime issues and expand the evidence base for policy and operational decisions’

• Normative work to assist States in the ratification and implementation of the relevant international treaties, the development of domestic legislation on drugs, crime and terrorism, and the provision of secretariat and substantive services to the treaty-based and governing bodies’

In short, the UNODC serves as a liaison between all states in the fight against transnational organised crime and the drug trade – it is also the main body assisting states in the ratification and implementation of international agreements and treaties.

The UNODC therefore does not mandate action in and of itself, operating in more of an advisory capacity to states in helping them resolve pertinent issues. Perhaps the most significant public output of the organisation are its reports; the UNODC produces an annual World Drug report, as well as a variety reports on the other issues it covers – including, for instance, crop monitoring surveys for countries and regions.

**INTRODUCTION**

Cybercrime is defined as a crime that is committed using a network-connected device such as a computer or a mobile phone. Those who commit [cyber-crime](https://en.wikipedia.org/wiki/Cybercrime) are known as cyber criminals or cyber crooks. With the growing digitization, internet crimes are also increasing at a faster pace.  As, this type of crime can be committed from a distant location; for an example-a foreign country, most criminals prefer this mode as the risk of getting traced and punished is limited.  Some common types of cybercrimes include phishing, [hacking](https://www.reveantivirus.com/en/computer-security-threats/computer-hacking), cyber-bullying, identity theft, spamming to name a few. Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. More serious crimes like cyberterrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.

Crimes that use computer networks to advance other criminal activities, which include drug trafficking. In today’s world, buying and selling of recreational drugs happen online in dark-net markets. Dark-net markets or cryptomarkets are commercial websites which operate by dark-nets or proxies such as Tor or I2P etc. The main function of these markets is black marketing and marketing by all other illegal modes. Drug traffickers generally use encrypted messaging tools to build communications with drug mules.

There have been several instances of dark web site, such as the site ‘Silk Road’ was a notorious online marketplace for drugs, before it was shut down by law enforcement. It got reopened again under new management, but got shut down again later on. Another site emerged later on with the same name just to use the brand value.

To take any measure to prevent illegal drug trafficking is not that easy, and when at the same time it happens by way of cyber crimes, it becomes more difficult, as cyberspace has no limits. Drug trade is international in nature, and law enforcement agencies are not always effective because of the wide and complex nature of cyber attackers. However, since the profit of drug trafficking and cyber crimes are equally big, mere one or two arrests here and there won’t bode any measure. International laws and partnerships across nations will have to be strong. One nation should help another in case of investigation or extradition of a criminal to the other. Overall, to neutralise drug trafficking by cyber crimes one nation’s law is never sufficient. These are the places where United Nations, or INTERPOL can come up with some measures.

**Forms of Cybercrimes**

For the purposes of this guidance note, Cybercrime can be defined across a range of offences which have been recognized by bodies such as Interpol, Europol, the Council of Europe, the European Union, the Asia‐Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS), the Commonwealth of Nations, the Group of Eight (G8), the Organization for Economic and Development Cooperation (OECD), to name but a few.

Computer crime, cybercrime, e‐crime, hi‐tech crime, electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Such crimes may be divided broadly into 2 types of categories: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

The former is the basic form of computer related offences, which are against the confidentiality, integrity and availability of computer data and system, including illegal access; interference with computer data and computer system; theft of data; interception of data in the computer system. Some examples include hacking, cracking, virus/worm attack, time or logic bombs, spyware malware and other malicious code, Trojan horses, web jacking , denial of service attacks, salami attacks, data diddling, and email bombing.

The latter is the expanded form of computer related offences, which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected by criminal law against attacks using traditional means. Examples include child sexual abuse and exploitation, economic fraud, forgery and identity theft, phishing scams, trafficking in human beings, illicit sales of controlled substances, terrorism, cyber‐stalking or harassment, cyber bullying, information warfare and intellectual property crimes.

Although there is no definitive list of what constitutes cybercrime or computer related crime, according to Broadhurst, a general consensus appears to have emerged about what falls within the scope of the offences that occur in cyberspace:

* Hacking an other forms of illegal access to computer systems;
* Illegal Interception of Telecommunications;
* Piracy Copyright Theft;
* Cyber Stalking;
* Electronic money laundering and Tax evasion;
* Electronic Vandalism, Use of the Internet for Terrorist Purposes, Denial of Service, Extortion;
* Sales and Investment Fraud, Forgery (Classic Pyramid schemes);
* Electronic Funds Transfer Fraud and Counterfeiting (Carding);
* Identity Theft and Misrepresentation;
* Espionage;
* Resource Theft ‐ illegal use of PC.
* Telecommunications Theft;

**Online drug trading**

The potential role of the Internet in facilitating drugs trade first gained mass attention with the rise and fall of Silk Road; the first major online market place for illegal goods on the hidden web. After Silk Road was taken down by the FBI in October 2013, it was only a matter of weeks before copycats filled the void.

Today, there are around 50 so-called cryptomarkets and vendor shops where anonymous sellers and buyers find each other to trade illegal drugs, new psychoactive substances, prescription drugs and other goods and services. But it is not just the obscure parts of the Internet where drugs are on offer. There are numerous web shops, easily found by search engines, which offer new psychoactive substances, often labelled as 'research chemicals'.

The Netherlands occupies a crucial position in European illicit drug markets. Data from the European Monitoring Centre for Drugs and Drug Addiction suggested it is the main producer of MDMA, ecstasy and herbal cannabis and a key distribution hub for cannabis resin and cocaine. Whether the pivotal role of the Netherlands also extends online, has yet been unclear.



**Findings**

* Compared to the days of Silk Road in 2013, the **number of transactions of illicit drugs on the cryptomarkets has tripled**, with **revenues doubling**. This is despite various law enforcement interventions and exit scams by online marketplaces, which have led to declining levels of trust between buyers and vendors, and less confidence in cryptomarkets.
* **Total drug revenues on cryptomarkets**(excluding prescription drugs, alcohol and tobacco) during January 2016 were estimated to be **between $12.0 (€10.5) million\* and $21.1 (€18.5) million\***. This suggests that cryptomarkets are only a niche market. According to the [European Monitoring Centre for Drugs and Drug Addiction](http://www.emcdda.europa.eu/)(EMCDDA), the total offline market for drugs is much larger, and is estimated to be $2.3 (€2) billion\* on average per month for Europe alone.
* There is evidence that drugs sold on cryptomarkets are fuelling offline drug markets, with buyers sourcing stock for offline distribution. **Twenty five per cent of total drug transactions on cryptomarkets during January 2016 were greater than $1,000 (€877.2)\***, making it likely that these drugs were bought for wholesale purposes. The majority of drugs sold on cryptomarkets were under $100 (€87.7)\*, so were likely to be for personal use, but they only generated 18 per cent of total transactions.
* **Illicit drugs sold on cryptomarkets were dominated by cannabis (37 per cent), stimulants (cocaine, amphetamines) (29 per cent) and ecstasy-type drugs (19 per cent).** This seems very similar to EMCDDA estimates about drugs sold offline, apart from ecstasy-type drugs (just three per cent of the total European retail drug market) and heroin (28 per cent of the total European drug market, but just six per cent of the total drugs sold on cryptomarkets).
* **Cryptomarkets appeared to be dominated by vendors from the U.S, Australia, Canada and Western Europe.** Vendors who indicated they were operating from the U.S. had the highest market share of drugs (35.9 per cent of total drug revenues), closely followed by the U.K. (16.1 per cent) and Australia (10.6 per cent). The Netherlands had a 7.1 per cent revenue share, which was less than Germany at 8.4 per cent.
* Per capita the Netherlands had the highest revenues for illicit drug sales on cryptomarkets – **Dutch vendors made $1,140,000 (€1 million)\* overall in January 2016**. The country dominated sales of MDMA and ecstasy on cryptomarkets – 23 per cent of global revenues of these drugs. Vendors who indicated they were operating from the Netherlands only had two per cent of global revenue sales of cannabis.

**Modes of Detection and Intervention**

The study identified four broad potential strategies that are available to law enforcement agencies in the detection and intervention of the Internet-facilitated drugs trade:

* traditional investigation techniques applied in the drug chain (e.g. surveillance, undercover operations)
* postal detection and interception (e.g. collaboration between law enforcement agencies and postal services)
* online detection (e.g. big data techniques, monitoring of online marketplaces, tracking money flows)
* online disruption (e.g. taking down online marketplaces).

In addition, international cooperation and coordination (and the accompanying legal challenges), capacity and resources and (technical) capabilities could play a facilitating role in deploying the different strategies to tackle Internet-facilitated drugs trade.

**UNODC ACTIONS AGAINST CYBERCRIME**

Cyber. It is the inescapable prefix defining our world today. From the privacy of individuals to relations between states, cyber dominates discussions and headlines - so much so that we risk being paralyzed by the magnitude of the problems we face.

But we would do well to keep in mind that despite the many outstanding questions on the future of cybersecurity and governance, international cooperation is essential to tackle the ever-growing threats of cybercrime.

Online exploitation and abuse of children. Dark-net markets for illicit drugs and firearms. Ransomware attacks. Human traffickers using social media to lure victims. Cybercrime's unprecedented reach - across all borders, into our homes and schools, businesses, hospitals and other vital service providers - only amplifies the threats.

A recent estimate put the global cost of cybercrime at 600 billion US dollars. The damage done to sustainable development and safety, to gender equality and protection -women and girls are disproportionately harmed by online sexual abuse - is immense.

Keeping people safer online is an enormous task and no one entity or government has the perfect solution. But there is much we can do, and need to do more of, to strengthen prevention and improve responses to cybercrime, namely:

Build up capabilities, most of all law enforcement, to shore up gaps, particularly in developing countries; and

Strengthen international cooperation and dialogue - between governments, the United Nations, other international as well as regional organizations, INTERPOL and the many other partners, including business and civil society, with a stake in stopping cybercrime.

Cyber-dependent crime, including malware proliferation, ransomware and hacking; cyber-enabled crime, for example email phishing to steal financial data; and online child sexual exploitation and abuse all have something in common besides the "cyber" aspect: they are crimes.

Police, prosecutors and judges need to understand these crimes, they need the tools to investigate and go after the criminals and protect the victims, and they need to be able to prosecute and adjudicate cases.

At the United Nations Office on Drugs and Crime (UNODC), we are working in more than 50 countries to provide the necessary training, to sharpen investigative skills, trace cryptocurrencies as part of financial investigations, and use software to detect online abuse materials and go after predators.

UNODC training - focused primarily on Central America, the Middle East and North Africa, Eastern Africa and South East Asia - is also helping to identify digital evidence in online drug trafficking, confront the use of the dark-net for criminal and terrorist purposes, and improve data collection to better address threats.

A critical foundation for all our efforts is international cooperation. Our work - which is entirely funded by donor governments - has shown that despite political differences, countries can and do come together to counter the threats of cybercrime.

We are also strengthening international cooperation through the Intergovernmental Expert Group, which meets at UNODC headquarters in Vienna.

Established by General Assembly resolution (67/189), the Expert Group brings together diplomats, policy makers and experts from around the globe to discuss the most pressing challenges in cybercrime today. These meetings demonstrate the desire and willingness of governments to pursue pragmatic cooperation, which can only help to improve prevention and foster trust.

As a next step, we need to reinforce these efforts, including by providing more resources to support developing countries, which often have the most new Internet users and the weakest defences against cybercrime.

Tech companies are an indispensable ally in the fight against cybercrime. We need to increase public-private sector engagement to address common concerns like improving education and clamping down on online abuse material.

Countering cybercrime can save lives, grow prosperity and build peace. By strengthening law enforcement capacities and partnering with businesses so they can be part of the solution, we can go a long way in ensuring that the Internet can be a force for good.

**ACTIONS BY UNODC TO COMBAT THE ISSUE**

**Global Programme on Cybercrime**

The complex nature of cybercrime, as one that takes place in the borderless realm of cyberspace, is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime, and their victims, are often located in different regions, and its effects ripple through societies around the world. This highlights the need to mount an urgent, dynamic and international response.

**Mandates**

According to General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, the Global Programme on Cybercrime is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance.

Prior to the commencement of the Global Programme, UNODC's open-ended intergovernmental expert group was established to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. This work includes the exchange of information on national legislation, best practice, technical assistance and international cooperation.

**Cybercrime Repository**

In 2015 UNODC under the framework of the Commission on Crime Prevention and Criminal Justice (CCPCJ) launched the cybercrime repository, a central database of legislation, case law and lessons-learned on cybercrime and electronic evidence. The cybercrime repository aims to assist countries in their efforts to prevent and effectively prosecute cybercriminals.

The repository comprises of three parts that aim to facilitate States' efforts against cybercrime:

* The Database of Legislation, which contains substantive and procedural legislation on cybercrime and electronic evidence of over 180 countries and is searchable by country, type of cybercrime offence and procedural aspects. The database contains extracts of laws relevant to cybercrime offences and cross-cutting issues and allows users to access full legislation documents;
* The Case Law Database, which contains jurisprudence, as well as records of successful law enforcement operations, on cybercrime and crimes related to electronic evidence. This allows users to see how States are tackling cybercrime cases both operationally and in their courts;
* The Lessons Learned Database, which contains national practices and strategies in preventing and combating cybercrime. Information compiled in this database has been gathered in the framework of the UNODC Comprehensive Study on Cybercrime and is supplemented by national cybercrime and cybersecurity strategies.

**Treaties & International Agreements on Cyber Crime**

**United Nations Convention Against Transnational Organized Crime (2000)**

This treaty, also known as the **Palermo Convention**, obligates state parties to enact domestic criminal offenses that target organized criminal groups and to adopt new frameworks for extradition, mutual legal assistance, and law enforcement cooperation.  Although the treaty does not explicitly address cyber crime, its provisions are highly relevant.

**Council of Europe Treaties**

**Convention on Cybercrime (2001)**

Also known as the Budapest Convention, this is the first international agreement aimed at reducing computer-related crime by harmonizing national laws, improving investigative techniques, and increasing international cooperation.

The COC comprises four chapters.1 The first chapter defines the terms. The second chapter specifies measures that need to be adopted at the national (domestic) level, including establishment of substantive criminal laws on offenses such as illegal access and interception, data and system interference, etc., the procedural laws, and jurisdictions over offenses. The third chapter contains principles of international co-operation such as extradition and mutual assistance. The last chapter allows participating countries to set the scope in terms of territorial application and reservation.

**Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003)**

State parties which have ratified this protocol to the Budapest Convention are obligated to enact laws to criminalize racist or xenophobic acts that are expressed or otherwise communicated online.

**CYBERCRIME LAW**

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters (UNODC, 2013, p. 52). Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law.

**Substantive law**

An illegal act needs to be clearly described in and prohibited by law. Pursuant to the moral principle of nullum crimen sine lege (Latin for "no crime without law") a person cannot be punished for an act that was not proscribed by law at the time the person committed the act (UNODC, 2013, p. 53). Substantive law  defines the rights and responsibilities of legal subjects, which include persons, organizations, and states. Sources of substantive law include statutes and ordinances enacted by city, state, and federal legislatures ( statutory law), federal and state constitutions, and court decisions.

|  |
| --- |
| **Did you know?**Some countries, instead of developing new special laws against cybercrime, amended their national legislation or codes, adding specific paragraphs to address cybercrime. With this practice, an interesting consequence for consideration has been that some countries decided to criminalize separately the illegal use of information and communication technology to commit any crime. Thus, if the perpetrator used illegal access in order to commit forgery or fraud, such behaviour would constitute two crimes at the same time. |

Substantive cybercrime law includes laws that prohibit specific types of cybercrime (described in Cybercrime[Module 2](https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/intro.html) on General Types of Cybercrime) and punishes non-compliance with these laws. Cybercrime includes traditional, real-world (offline) crimes (e.g., fraud, forgery, organized crime, money-laundering, and theft) perpetrated in cyberspace that are 'hybrid' or 'cyber-enabled' crimes, as well as 'new' or 'cyber-dependent' crimes that have been made possible with the advent of the Internet and Internet-enabled digital technologies (Wall, 2007; Maras 2014; Maras, 2016). For these reasons, many countries have developed laws that are specifically designed to deal with cybercrime. For example, Germany, Japan, and China, have amended the relevant provisions of their criminal code to combat cybercrime. Countries have also used existing laws that were designed for real-world (offline) crime to target certain cybercrimes and cybercriminals. As another example, in Iraq, the existing civil code (Iraqi Civil Code No. 40 of 1951) and penal code (Iraqi Penal Code No. 111 of 1969) are used to prosecute real-world crimes (e.g., fraud, blackmail, identity theft) perpetrated via the Internet and digital technology.

|  |
| --- |
| **Legal systems**Each state has its own legal system, which affects the creation of substantive criminal law on cybercrime. These systems include (Maras, forthcoming, 2020):1) Common law. These systems create laws by legal precedent (i.e., ruling in case binding to the court and lower courts) and established practice. These laws exist as separate laws and case law (i.e., law that develops from court decisions or legal precedent).2) Civil law. These legal systems have codified, consolidated, and comprehensive legal rules or statutes that delineate basic rights, responsibilities, duties and expectations of behaviour. These legal systems are primarily based on legislation and constitutions.3) Customary law. These legal systems include established and accepted patterns of behaviour within a culture that are perceived by those within the culture to be law ( opinion juris). In international law, customary law governs relationships and practices between states and is considered binding for all states.4) Religious law. These legal systems include rules derived from religion or the use of religious documents as a legal source and authority.5) Legal pluralism. In this type of legal system, two or more of the above-mentioned legal systems (i.e., common, civil, customary or religious law) may exist. |

Substantive law focuses on the substance of crime, such as the elements of a crime which includes the prohibited conduct ( actus reus - "guilty act") and the mental element ( mens rea - "guilty mind"). Different states may choose to criminalize different conduct by choosing different elements that constitute a crime. Alternatively, states may criminalize the same conduct, but the laws may still differ as to what "state of mind" makes them culpable for their conduct (i.e., level of criminal culpability). To this end, laws that criminalize, for example, unauthorized access to computer systems and data vary between countries, depending on the degree of intent held by a purported criminal (see "Levels of Criminal Culpability" box below).

|  |
| --- |
| **Levels of criminal culpability**There are different levels of criminal culpability (or criminal responsibility) based on the degree to which an illicit act was intentional (purposely or wilfully committed) or unintentional (recklessly and negligently committed) that varies according to legal system (Simons, 2003; Dubber, 2011; Maras, 2020):Purposely. A person purposely commits crime when the person is acting to cause harm (i.e., the person has intent to cause harm). A case in point is the UK Computer Misuse Act of 1990, which criminalizes, among other things, unauthorized access to systems and data with the intention of causing changes and/or damage, disruptions of systems and services, and modifications of system data and programmes.Wilfully. A person wilfully commits crime when the person is aware that an action will cause harm but commits the harm or wrongdoing anyway. A person can be charged pursuant to the US Computer Fraud and Abuse Act of 1986, specifically 18 U.S.C. § 1030(a)(1), forhaving knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.Recklessly. An individual recklessly commits crime when the person engages in an act even though the person is aware of the substantial and unjustifiable risk of harm to others but shows disregard for or indifference to the risk of harm. In Australia, a person can be charged under Division 477.2(1)(c) of Cybercrime Act 2001 (No. 161, 2001) if a "person is reckless as to whether the [unauthorized] modification [of data] impairs or will impair: (i) access to that or any other data held in any computer; or (ii) the reliability, security or operation, of any such data."Negligently. Negligence is the lowest level of culpability. Those engaging in negligent behaviour lack awareness of the negative consequences of an act. In Senegal, "[a]nyone who, even through negligence, processes or arranges the processing of personal data without having complied with the formalities set out in the Law on Personal Data prior to using such data shall be punished" (Article 431-17, Law No. 2008-11 on Cybercrime).**Note:** Levels of criminal culpability are not universal (Fletcher, 2000, p. 445-446, cited in Ohlin, 2013 p. 82). |

**Procedural law**

Procedural law demarcates the processes and procedures to be followed to apply substantive law and the rules to enable the enforcement of substantive law. An important part of procedural law is criminal procedure, which includes comprehensive rules and guidelines on the manner in which suspected, accused, and convicted persons are to be handled and processed by the criminal justice system and its agents (Maras, forthcoming, 2020; for general information about criminal procedure, see LaFave et al., 2015; for information about international criminal procedure, see Boas, et al., 2011). Ultimately, procedural cybercrime law includes provisions on jurisdiction and investigative powers, rules of evidence and criminal procedure that relate to data collection, wiretapping, search and seizure, data preservation and data retention (Cybercrime presents certain unique challenges regarding procedure, especially with respect to jurisdiction, investigations, and digital evidence.)

Jurisdiction. Law enforcement may only carry out a cybercrime investigation, and national courts may only adjudicate cybercrime cases, if the interested state has jurisdiction. Jurisdiction refers to a state's power and authority to enforce laws and punish noncompliance with laws (this topic is discussed in further detail in Cybercrime [Module 7](https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/intro.html) on International Cooperation against Cybercrime). Jurisdiction is linked to state sovereignty, which is a country's right to exercise authority over its own territory (UNODC, 2013, p. 55). Jurisdiction is commonly associated with geographic territory or locus commissi deliciti (the place where the crime was committed), whereby states claim jurisdiction over and prosecute crimes committed within their territory (principle of territoriality). Given that there are no geographic boundaries and territories in cyberspace, the location cannot be used to determine jurisdiction. For this reason, states rely on a multitude of other factors to determine jurisdiction (Brenner and Koops, 2004; Rahman 2012; Maras, forthcoming, 2020): One such factor is the nationality of the offender ( principle of nationality; active personality principle). This principle holds that states have the authority to prosecute their nationals even if these nationals are outside of their territory. To a lesser extent (in its use) the nationality of the victim can be used to assert jurisdiction over a crime ( principle of nationality; passive personality principle). A state can further establish jurisdiction because crime committed in another state (e.g., treason or espionage) impacted the interests and security of the state seeking jurisdiction over the case ( protective principle).

Investigative measures and powers. Digital evidence of cybercrimes presents particular challenges both in terms of its handling and use in court proceedings. According to the 2013 [UNODC Draft Comprehensive Study on Cybercrime](http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf), "[w]hile some of these investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving…[digital] data storage and real-time data flows" (p. 122), thus requiring specialized powers for the investigation (UNODC, 2013, p. 54). These specialized powers are prescribed by law and cover not only access to information needed but also include safeguards to ensure that the data is obtained pursuant to appropriate legal orders and accessed only to the extent necessary and authorized by law.

**Preventive law**

Preventive law focuses on regulation and risk mitigation. In the context of cybercrime, preventive legislation seeks to either prevent cybercrime or, at the very least, mitigate the damage resulting from the commission of a cybercrime (UNODC, 2013, 55). Data protection laws (e.g., the EU [General Data Protection Regulation](https://gdpr-info.eu/) of 2016, and the [African Union Convention on Cyber Security and Personal Data Protection](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf) of 2014, discussed in Cybercrime[Module 10](https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/index.html) on Privacy and Data Protection) and cybersecurity laws (e.g., [The Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine](http://cis-legislation.com/document.fwx?rgn=101792) of 2017) are designed to lessen the material harms from criminal breaches of private data should a cybercrime occur, and/or minimize private vulnerability to cybercrime. Other laws enable criminal justice agents to identify, investigate, and prosecute cybercrime by ensuring the necessary tools, measures, and processes are in place to facilitate these actions (e.g., telecommunications and electronic communications service providers' infrastructure is such that it enables wiretapping and data preservation).

**Questions to Consider:**

Q1 What are the existing forms of cyber crime and the means to detect them?

Q2 Does your country have any cyber legislature? How efficient has it proven to be in dealing with cyber crimes?

Q3 Is the existing international legal regime capable with dealing with the increasing cyber threats? If not, which areas is it lacking in?

Q4 What are the ways to dismantle the online drug market?

Q5 How can we track the cryptocurrency used for the transactions?

Q6 How can UNODC’s Cybercrime Repository be better utilized?

Q7 Given that there are no geographic boundaries in cyberspace, how do we determine jurisdiction in cases?

Q8 What role can the private sector including tech giants play?

Q9 What kind of preventive law can be introduced to resolve the issue?

**Research Links**

* <https://www.rand.org/pubs/research_reports/RR1607.html>
* <https://www.cybercrimelaw.net/Cybercrimelaw.html>
* <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx>
* <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>
* <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.8982&rep=rep1&type=pdf>
* <https://www.sascv.org/ijcjs/pdfs/LIijcjs2017vol12issue2.pdf?fbclid=IwAR1ccAjj15WrpA-4esFDcGwjBYRXb4rQulWgWi_FGADq14gSl8QamPozpv4>
* <https://snpf.org/wp-content/uploads/2015/09/Drug-related-cybercrime-and-associated-use-of-the-internet.pdf?fbclid=IwAR2UZH-IjrBDSxQLhFtLsHAJtT-abTQ2gIOAfT6zNenRETytNeQqO5PSHIw>