SPECIAL RULES
SECURITY COUNCIL
VOTING AND MAJORITIES

1. For voting on Substantive Matters an affirmative vote of nine Members of the Security Council including the votes of the five Permanent Members shall be needed.
2. For voting on Procedural Matters the general rules of other committees apply.

Appendix 1.1: THE PRECEDENCE OF POINTS AND MOTIONS

As for the precedence of motions, the most disruptive one shall be voted upon as the first one. In case that a Motion with the higher precedence passes, the rest of the Motions are automatically considered to be ruled out and the committee will not vote upon them anymore.

In order at any time, including speeches and Voting Procedure

1. Point of Personal Privilege
2. Point of Order
3. Point of Parliamentary Inquiry (not in order during speeches)

In order when the Floor is open:

1. Motion for Closure of the Debate
2. Motion to Table the Debate
3. Motion for Adjournment of the Meeting
4. Motion for Suspension of the Meeting
5. Motion to Resume Debate
6. Motion to Introduce an Amendment
7. Motion to Introduce a Working Paper
8. Motion for Un-moderated Caucus (its Extension has precedence)
9. Motion for Moderated Caucus (its Extension has precedence)
10. Motion to Change the Speaking Time
11. Motion to Open the Speaker´s List

In order after the Closure of the Debate:

1. Motion to Reorder Draft Resolutions
2. Motion to Divide the Question
3. Motion for the Roll Call

HIT MUN

From the Desk of the Bureau,

Honourable Member State Representatives,

It gives me immense pleasure in welcoming you all to the simulation of United Nations Office on Drugs and Crime (UNODC) at the HIT Model United Nations conference. We will be simulating the Commission on Crime Prevention and Criminal Justice (CCPCJ).

The agenda for this session is 'Preventing and Combatting Cybercrime'. The agenda, is of utmost significance in pertinence to the surge in cybercrime and cyber warfare in the current global scenario.

It is advised that the delegates go through the background guide thoroughly. The document will aid your research. The aim of the study guide is to provide clarity regarding the various aspects of the agenda as well as providing direction and to channelize your research. However, it is to be noted that this guide is not an all-encompassing source of information. This study guide has been prepared to give you a basic knowledge of the agenda and we strongly recommend that you research on various aspects on your own and try to gain an insight into the details of the agenda.

We will be following the UNA-USA rules of procedure in this committee. Those who are not well versed with these rules of procedure are requested to have a look at it before the committee begins.

Feel free to drop your queries at :

Chairperson:

Kumar Saurabh (saurabh5881@gmail.com)

Vice-Chairperson:

Anomitra Paul (anomitra.artimona.pl@gmail.com)

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)

ABOUT THE COMMITTEE

Commission on Crime Prevention and Criminal Justice

The Economic and Social Council is one of the principal organs of the United Nations. It sets up commissions in economic and social fields and for the promotion of human rights, and such other commissions as may be required for the performance of its functions (Article 68 of the United Nations Charter).

Thus, in its resolution 1992/1, upon the request of the General Assembly in its resolution 46/152, the Economic and Social Council established the Commission on Crime Prevention and Criminal Justice as one of its functional commissions, which also acts as a subsidiary body.

Functions

The Commission on Crime Prevention and Criminal Justice meets every year in Vienna. It is the principal policymaking body within the United Nations system on crime prevention and criminal justice issues.

In accordance with the "Statement of principles and programme of action of the United Nations crime prevention and criminal justice programme", contained in the annex to General Assembly resolution 46/152, the Commission has the following functions:

- To provide policy guidance to the United Nations in the field of crime prevention and criminal justice.
- To develop, monitor and review the implementation of the crime prevention and criminal justice programme.
- To facilitate and help to coordinate the activities of the institutes for the prevention of crime and treatment of offenders, affiliated to the United Nations.
- To mobilize the support of Member States for the programme.
- To prepare for United Nations congresses on crime prevention and criminal justice.
- To consider suggestions regarding possible subjects for the programme of work.

In addition to strategic management, budgetary and administrative questions, during its regular session, the Commission considers a number of standing items, including:

• The integration and coordination of efforts by the United Nations Office on Drugs and Crime and by Member States in the field of crime prevention and criminal justice, as well as United Nations standards and norms;
• Global crime trends and emerging issues and responses in the field of crime prevention and criminal justice;
• Matters relating to previous United Nations congresses and upcoming ones.

In its resolution 46/152, the General Assembly decided that the United Nations crime prevention and criminal justice programme would provide States with practical assistance, such as data collection, information- and experience-sharing and training, to prevent crime within and among States and to improve responses to it.
Moreover, in its resolution 61/252, the General Assembly enabled the Commission to approve the budget of the United Nations Crime Prevention and Criminal Justice Fund.

Unique Characteristics

One of the distinctive features of the work of the Vienna-based commissions, namely the Commission on Crime Prevention and Criminal Justice and the Commission on Narcotic Drugs, is the application of the Vienna consensus, an informal practice used in negotiations on draft resolutions.
The Vienna consensus promotes extensive negotiations on each resolution and encourages commitment from all parties involved to achieve the support of all States and to adopt resolutions on the basis of consensus.
A voting procedure is, in principle, possible, as provided for in rule 57 of the rules of procedure of the functional commissions of the Economic and Social Council. It is, however, not regularly used, in the light of the Vienna consensus and the spirit of cooperation among Member States.

Participation:

Participation is governed by the rules of procedure of the functional commissions of the Economic and Social Council, which apply to all the subsidiary bodies established by the Council.
Aside from Commission members, non-Member States and non-governmental organizations can attend. Other participants include the centres and institutes that are part of the United Nations crime prevention and criminal justice programme network, and special rapporteurs of the Human Rights Council on issues of relevance to the work of the Commission.

Member states of the commission

The Commission is composed of 40 States members. The distribution of seats follows common and usual practice within United Nations bodies, and is done on a regional basis (12 for Africa, 9 for Asia, 8 for Latin America and the Caribbean, 4 for Eastern Europe and 7 for Western Europe and other States). According to General Assembly resolution 46/152 and Economic and Social Council resolution 1992/1, half of the membership is elected for a term of three years.

Non-member States:

Member States that are not members of the Commission can take part in the proceedings. While there are a number of restrictions for non-members, a large number of Member States that are not members of the Commission usually participate in its sessions.

Member States that are not members of the Commission do not have the right to vote. They are, however, able to submit proposals that may be put to the vote on request of any member of the Commission or of the subsidiary organ concerned.

Non-members also engage in informal negotiations on resolutions that are adopted by way of the Vienna consensus. The seating arrangements reflect the composition of the Commission: its members are seated at the front of the conference room, in alphabetical order, followed by non-members and other observers at the back of the room.

Non-governmental organizations:

Non-governmental organizations having consultative status with the Economic and Social Council of the United Nations are also present at the Commission.

They may designate authorized representatives to sit as observers at public meetings of the Commission and its subsidiary organs. Moreover, the Commission may consult with such organizations, and they are usually heard by the Commission after Members have spoken.

Outcome documents:

The main outcomes of the Commission are the resolutions, as is the case for the majority of the intergovernmental bodies of the United Nations. Virtually all the resolutions are adopted by consensus. If no consensus is reached, the proposed text is usually subject to negotiations until agreement is reached or the text is withdrawn.

The Commission may also recommend draft resolutions either for adoption by the Economic and Social Council or for approval by the Council and subsequent adoption by the General Assembly. All the resolutions and decisions adopted or recommended by the Commission are brought to the attention of the Economic and Social Council through reportsadopted by the Commission at the end of each session. The reports also include summaries of the deliberations that took place.

Structure and conduct of work:

The work of the Commission is governed by the Rules of Procedure of the Functional Commissions of the Economic and Social Council . The structure of the work of the Commission is outlined as follows:

• The reconvened session of the Commission is usually held in December to consider strategic management, budgetary and administrative questions. At the end of the reconvened session, the following session is opened for the purpose of electing its Bureau.

• The Bureau of the Commission is composed of a Chair, three Vice-Chairs and a Rapporteur. These officers of the Bureau are elected based on the principle of equitable geographical distribution.

• A group composed of the Chairs of the five regional groups, the Chair of the Group of 77 and China, and a representative of or observer for the State holding the Presidency of the European Union assists the Chair of the Commission.

• Pre-session consultations usually take place on the last working day before the start of the regular session of the Commission.

• The regular session of the Commission takes place in Vienna over five days towards the end of the first part of the year (usually in May).

• At the beginning of the regular session, the Commission adopts its agenda and programme of work.

• The Commission also holds a discussion on a theme, with introductory statements and statements from representatives of Member States, observers and expert panellists.

• Action on agenda items involves the adoption of resolutions, which are the main outcomes of each session, and of decisions, which for the most part deal with procedural matters.

As in other intergovernmental bodies of the United Nations and in accordance with established practice, the Commission first considers draft resolutions in the Committee of the Whole. This Committee meets in parallel with the plenary before such proposals are submitted to the plenary for adoption in the last day of the session. No debate or discussion on any proposal can take place before copies of such a document are circulated among Member States, although informal consultations normally take place before that.

Cybercrime

Cybercrime is an evolving form of transnational crime.

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

What is cybercrime?

There is no international definition of cybercrime or cyberattacks. Offences typically cluster around the following categories:

Offences against the confidentiality, integrity and availability of computer data and systems;

- Computer-related offences;
- Content-related offences;
- Offences related to infringements of copyright and related rights.

Broadly, cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse.

- Cyber-dependent crime requires an information and communications technology infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).
- Cyber-enabled crime is that which can occur in the offline world but can also be facilitated by information and communications technology. This typically includes online frauds, purchases of drugs online and online money laundering.
- Child sexual exploitation and abuse includes abuse on the clear internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion - known as "sextortion".

Combating cybercrime and the Sustainable Development Goals:

While there is no specific Sustainable Development Goal to address cybercrime, it can be seen as an obstacle to achieving a number of targets, such as those under Goal 16, which relate to violence and other forms of crime, such as corruption and arms trafficking (Targets 16.1, 16.4, 16.5).

In addition, certain criminal activities can be facilitated by information and communications technology, such as the recruitment of victims of trafficking in persons (target 10.8) or sexual exploitation of women, which would characterize a form of violence against women (target 5.2).

By choosing to have cybercrime as a Model United Nations issue, participants can:

• Obtain more knowledge about the different phenomena relating to cybercrime, such as cyber-dependent, enabled and specific crime types;

• Increase their understanding of Member States' efforts to address cybercrime in intergovernmental fora;

• Increase their knowledge of best practices and ways in which Member States and society can cooperate to address cybercrime.

Definition of Key Terms

The Internet:

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide.

World Wide Web:

A platform for online communications through the Internet, allowing people to share and access information from all over the world.

Digital Age:

The Digital Age is an era of human history based on information computerization. The Digital Age is associated with the Digital Revolution, which refers to the growing number of people connected online in the world.

Hacking:

The act of using technology (most often computers) to gain unauthorized access to data in a system belonging to a person, company or country.

Virus:

A type of computer code, which has the ability to copy itself and spread on the computer, corrupting the system or destroying data.

Malware:

Computer software or programs designed to damage or block computers. Firewall A protection system for computers to prevent unauthorized access.

Cyber Security:

"Information security as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole."

Cyber Security Attacks:

Breaking into the cyber security systems to acquire private information. This action can happen on a personal level up to on a macro level, and is illegal in most places.

Cyber Security Strategies :

Strategies and methods used to prevent and limit the number of cyber security attacks and breaches. This consists of a wide variety of methods, security concepts, policies and tools, to be discussed later.

Cyber Security Standards:

Security standards that enable organizations to practice safe security techniques to minimize the number of successful cybersecurity attacks. These guides provide general outlines as well as specific techniques for implementing cybersecurity.

Cybercrime:

Hacking into servers with the intent to gain economic benefits, i.e. bank account, monetary funds, etc.

Cyber Warfare :

Hacking into servers with the intent of acquiring political information, i.e. confidential government information, access to weaponry.

General Overview :

Cyber attackers have many advantages in carrying out their illegal activity without any form of impediment, for example: the law enforcement and jurisdiction finds it difficult to locate where cyber attacks take place. Therefore, it is by no means clear who the cybercriminals are, meaning that they can't be easily identified. Furthermore, it is financially uncomplicated to engage in activity within the cyberspace, consequently one can master its tools and use it against the state. In the past cyber crime was committed mainly by individuals or small groups. Today we see highly complex cybercriminal networks bringing together individuals from across the globe to perpetrate crimes on an unprecedented scale.

Cybercrimes can be more harmful than traditional ones, since cyber offenders can situate multiple attacks at any time, from anywhere, anonymously against information systems. Besides, since organizations become aware of unlawful use of electronic devices through information systems and electronic monitoring, a well-developed cyber-attack can cover its own traces. Cybercrimes can also damage critical infrastructure and other hardware structures. Criminal organizations turning to the internet to facilitate their activities and maximize their profit in minimal time. These crimes aren't necessarily new, such as theft, fraud, illegal gambling, scale of fake medicines which can be labelled as darknet markets. These are evolving with the increase of opportunities presented before them. Commercial service is also a key aspect of cybercrime, it essentially means the exchange of goods. However, in the Dark Web, the goods mentioned are illicit. The bitcoin currency used for these transactions doesn't require the government's or bank's approval, instead, there are "miners" (a network of users) which control and verify these transactions. Therefore, bitcoin is a service that serves practical purposes in enabling the Dark Web to be usable as they are uninsured and very difficult to track back to the person who spent them. Whenever a bitcoin transaction transpires, only the wallet ID is recorded, not the names of the buyers and the sellers. This emphasises the anonymity of cybercrime. Additionally, another enabling mechanism of cybercrime is the Hidden Wiki, this site contains a catalogue of all the Dark Web Sites that are currently operating, user feedbacks on those sites, and information about what can be accessed through each site. Pedophilia on the dark web works like a darknet market too. Similar to a drug darknet market, pedophile pictures can be bought in exchange for bitcoins. However, the Dark Web also offers publishing and discussion forums for pedophiles. There are two types of pedophiles on the dark web: a division contribute to this illegal activity by using its content, but are not active outside of the web, and others, who are active in finding new ways to live their sexual attraction. The Onion Routing Project (TOR) is a free software first created by the US Naval Research Laboratory. It does not provide anonymity in itself, but it allows the exchange of information between two different entities to be anonymous. It is crucial to know that TOR is the key to the Dark Web. One use of TOR is that It helps journalists get in contact with whistleblowers or victims that prefer their identity to be anonymous. It also allows people working for NGO's to work without being traced. Debates on cybercrime are created to try and compromise the usage of The World Wide Web, more so to try to demote and eradicate unsafe and illegal activity in the cyberspace. However, there is a "freedom" factor that should be taken into consideration. The internet shouldn't be entirely restricted as users necessitate freedom of expression, along with having their personal information protected.

. Balancing the two requirements can come across as unattainable, also due to the fact that cybercrime has become a recently developed way to obtain money as cybercrime schemes remain inexpensive and accessible to anyone with criminal intent.

Major Parties Involved

European Commission:

The European Commission established a Communication on a European Cybercrime Centre in 2012 which has four main aims: 1. Serve as the European cybercrime information focal point; 2. Pool European cybercrime expertise to support Member States; 3. Provide support to Member States' cybercrime investigations; 4. Become the collective voice of European cybercrime investigators across law enforcement and the judiciary

The Onion Routing (TOR):

A software that creates a connection between several computers at a time that facilitates to hide an encryption. That implies that the start and end point of information traveling through the dark web remains unknown. The Onion Routing can be used for illegal purposes such as darknet markets, but also enables the right to anonymity.

International Criminal Police Organisation (Interpol) :

The International Criminal Police Organization, more commonly known as Interpol, is the international organization that facilitates international police cooperation. As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level.

The Asia-Pacific Economic Cooperation (APEC):

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime.

Internet Corporation for Assigned Names and Numbers:

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for the IP-addresses on the Internet. ICANN is responsible for the assignment, country code and server management functions. This gives ICANN full control over the Domain Name System (DNS), which basically controls content representation on the Internet. As ICANN is incorporated under the US law it is criticized for acting as the mean for the US to control the web. However, the existence of the Regional Internet Registries (RIR) controlling ICANN as well as the seven keys around the world given to online security experts ensure that ICANN does not abuse its power.

The National Crime Agency (NCA) :

The National Crime Agency is a national law enforcement agency in the United Kingdom. It was established in 2013 as a non-ministerial government department, replacing the Serious Organised Crime Agency and absorbing the formerly separate Child Exploitation and Online Protection Centre as one of its commands.

Global Cybersecurity Index (GCI) :

Multi-stakeholder initiative to measure the commitment of countries to cybersecurity. Each country's level of development will therefore be analysed taking into consideration five categories: legal measures, technical measures, organizational measures, capacity building and cooperation. Cybersecurity has a large scope of application that spreads across many industries and sectors. It is a survey that measures the commitment of member states in order to raise awareness.

Global Commission on Internet Governance The Global Commission on Internet Governance (GCIG):

It provides recommendations and practical advice on the future of the Internet. Its primary objective was the creation of "One Internet" that is protected, accessible to all and trusted by everyone. In their last report the Commission finalised courses of action that everyone needs to take to attain a more open and secure internet.

United States of America (USA):

The power that countries have over the Internet is crucial as cyber-governance links directly to cybersecurity and cybercrime. According to the Global Cybersecurity Index the USA is best prepared for any eventuality regarding a Cyberattack. The USA not only has the power to defend itself against cybercrime, but also the power it had to control the Internet in the past through ICANN (previously mentioned). Pressure from the international community led a slow separation between USA and ICANN assured by the "Affirmation Commitments" in 2009. However, in 2013 Snowden's revelations about NSA surveillance over the Internet contradicted these documents. Shortly after that, the US government announced that it would give up state control of ICANN.

The International Telecommunication Union (ITU):

The ITU is the United Nations specialized agency for information and communication technologies. ITU takes a human rights approach on the issue of cyber-security. Its vision and aim is to connect all citizens around the world through the World Wide Web. Hereby they fight for the right of access to the Internet. According to ITU's statistics Europe, North America (USA and Canada), Brazil and the Commonwealth nations are most committed to cyber-security. Furthermore, ITU provides guidelines and information related to cyber security.

General challenges:

Reliance on ICTs:

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or email communications. ICTs are now responsible for the control and management functions in buildings,cars and aviation services.The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures.Even short interruptions to services could cause huge financial damages to e-commerce businesses.

Number of users:

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2010. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth. With the growing number of people connected to the Internet, the number of targets and offenders increases.It is difficult to estimate how many people use the Internet for illegal activities.

Availability of information:

The Internet has millions of webpages of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia,an online encyclopaedia where anybody can publish.726 The success of the Internet also depends on powerful search engines that enable users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. "Googlehacking" or "Googledorks" describes the use of complex search-engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password protection systems.

Missing mechanisms of control :

All mass communication networks – from phone networks used for voice phone calls to the Internet – need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and even transnational communication infrastructure. The Internet also needs to be governed by laws, and lawmakers and law-enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

International dimensions:

Many data transfer processes affect more than one country. The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked. Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to the final destination. Further, many Internet services are based on services from abroad, e.g. host providers may offer webspace for rent in one country based on hardware in another.If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law-enforcement agencies in all countries affected. National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities. Cyber-crime investigations need the support and involvement of authorities in all countries involved. It is difficult to base cooperation in cybercrime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law-enforcement agencies often hinder investigations.

Transnational Nature:

Independence of location and presence at the crime site Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyberof-fences are transnational. International cybercrime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cybercrime legislation.Preventing "safe havens" is one of the key challeng-es in the fight against cybercrime. While "safe havens" exist, offenders will use them to hamper investigation. Developing countries that have not yet implemented cybercrime legislation may become vulnerable, as criminals may choose to base themselves in these countries to avoid prosecution. Serious offences affecting victims all over the world may be difficult to stop, due to insufficient legislation in the country where offend-ers are located. This may lead to pressure on specific countries to pass legislation. One example of this is the "Love Bug" computer worm developed by a suspect in the Philippines in 2000,756 which infected millions of computers worldwide. Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalized in the Philippines.

Previous Attempts to Resolve the Issue

 The world Summit on the Information Society (WSIS) was a conference held, sponsored by the United Na-tions, which covered the topics of : information, communication and in information society. One of its objec-tives was to unite the global digital divide separating rich countries from poor countries by extending internet access to LEDCs. In fact, this society formulated a resolution on the 12 December 2003 in Geneva which tar-geted cybercrime and the dark web.

 One of the largest and most infamous Dark Web marketplaces was Silk road. It was created in 2011 by Ross William Ulbricht , he obtained $13 million from allowing vendors to use his Silk Road Platform. The platforms not only sold drugs, but anything and everything that vendors put online. In October 2013, FBI discovered who was under Silk Road and finally shut it down. They concluded that over $1.2 billion sales had occurred which entailed 150,000 customers and 4000 vendors. This crisis depicts that illegal trade is a gargantuan business on the Dark Web.

 The United Nations Office on Drugs and Crime (UNODC) has worked 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 materialise and go after predators. As a result of this, a high-risk paedophile which had around 80 victims was arrested, tried and convicted. The training is carried out in partnership with the International Centre for Missing and Exploited Children and Facebook. This training is mainly focused in Central America, Eastern Africa and South-East Asia.

 Also, the UN has launched child sexual abuse reporting portals working with the Internet Watch Foundation, so that citizens can report images to prevent online exploitation

Further References:

https://www.unodc.org/unodc/fr/cybercrime/index.html
https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views
https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/07/Information-Security-Fact-Sheet-July2018.pdf
https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf
https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf
https://www.cambridge.org/core/services/aop-cambridge-core/content/view/02314DFCFE00BC901C95FA6036F8CC70/S2398772317000575a.pdf/sovereignty_in_the_age_of_cyber.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071
https://www.ispionline.it/en/pubblicazione/enhanced-cooperation-cybercrime-case-protocol-budapest-convention-20964