NMUN•NY 2019

14-18 April 2019

Documentation of the Work of the Commission on Crime Prevention and Criminal Justice

Conference B

Commission on Crime Prevention and Criminal Justice

Committee Staff

Director	Samantha Hall
Assistant Director	Anna Rickert
Chair	Ameya Patkar
Rapporteur	Adam Craig

Agenda

I. Criminal Justice Responses to Cybercrime in All Its Forms

II. Improving Coordination in Preventing and Combating Migrant Smuggling

III. Restorative Justice in Criminal Matters

Resolutions adopted by the Committee

Code	Topic	Vote
CCPCJ/1/1	Criminal Justice Responses to Cybercrime in All Its Forms	29 yes, 1 no, 1 abstention
CCPCJ/1/2	Criminal Justice Responses to Cybercrime in All Its Forms	Adopted by acclamation
CCPCJ/1/3	Criminal Justice Responses to Cybercrime in All Its Forms	Adopted by acclamation
CCPCJ/1/4	Criminal Justice Responses to Cybercrime in All Its Forms	Adopted by acclamation
CCPCJ/1/5	Criminal Justice Responses to Cybercrime in All Its Forms	Adopted by acclamation
CCPCJ/1/6	Criminal Justice Responses to Cybercrime in All Its Forms	Adopted by acclamation

Summary Report

The Commission on Crime Prevention and Criminal Justice held its annual session to consider the following agenda items:

I. Criminal Justice Responses to Cybercrime in All Its Forms
II. Improving Coordination in Preventing and Combating Migrant Smuggling
III. Restorative Justice in Criminal Matters

The session was attended by representatives of 31 Member States.

On Sunday, the committee adopted the agenda of I, II, III, beginning discussion on the topic of “Criminal Justice Responses to Cybercrime in All Its Forms.” By Tuesday, the Dais received a total of six proposals covering a wide range of sub-topics, addressing the dangers of the dark web, fraud in the financial sector, and national legislation to develop legal frameworks. Consistently, many delegations stressed the importance of equal access to justice and collaboration opportunities for all Member States to respond forcefully and effectively to the universal threat of cybercrime.

On Wednesday, six draft resolutions had been approved by the Dais, three of which had amendments. The committee adopted six resolutions following voting procedure, five of which received unanimous support by the body. The resolutions represented a wide range of issues, including increased cooperation on addressing cybercrimes related to child exploitation and the augmented support of educational scholarships for cybersecurity programs in developing Member States. Over the course of the week, the working atmosphere was productive and inclusive. Delegates made significant progress in finding solutions for the topics at hand.

National Model United Nations • NY

Code: CCPCJ/1/1
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrime in All Its Forms

---

The Commission on Crime Prevention and Criminal Justice,

Cognizant of the over 4.1 billion people with access to the internet according to the World Internet User Statistics of 2019, and with special regard to the growing number in developing countries,

Guided by the necessity to address cybersecurity multilaterally as is especially required by the transnational nature of many cybercrimes as noted in the United Nations (UN) Commission on Crime Prevention and Criminal Justice (CCPCJ) resolution 20/7 on "Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building,"

Recalling the need to strengthen the United Nations (UN) Crime Prevention and Criminal Justice program, in particular its technical cooperation capacity, as described in General Assembly resolution 67/189 on "Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity,"

Further emphasizing the role technical knowledge and capacity-building play in the global fight against cybercrime as presented in the 2010 *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*,

Reaffirming the work towards combating the malicious use of cyberspace as outlined in the objectives of Goal 16 of the Sustainable Development Goals,

Recognizing the creation of the International Telecommunication Union's Global Cybersecurity Agenda of 2007 in order to engage in international cooperation and broaden confidence and security protocols in the world of cyberspace,

Bearing in mind the cooperation at multilateral levels in the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information as promoted by General Assembly resolution 58/32 on "Developments in the field of information and telecommunications in the context of international security,"

Stressing the need for more adequate efforts to facilitate the transferring of informational technology and capacity-building to developing countries, specifically to Member States and developing nations, in areas of cybersecurity and educational development training as outlined initially in General Assembly resolution 58/199 on "Creation of a global culture of cybersecurity and the protection of critical information infrastructures,"

Acknowledging that developing nations face a loss of technical knowledge through the international emigration of skilled persons as evidenced in the UN Conference on Trade and Development's The Least Developed Countries Report 2007 and as recognized in General Assembly resolution 67/189 on "Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity" that this loss of technical knowledge disadvantages the capacity of these states to combat cybercrimes,

Reaffirming the work done by the African Union 2014 *Convention on Cyber Law and Personal Data*, particularly as it relates to the rising prominence of cyberspace in developed and developing countries and the importance of creating a lasting framework that protects the privacy and rights of all people,

1. *Recommends* Member States to create the Cybersecurity for All States Taskforce (CAST), an international expert group hoping to help less developed states build cyber security infrastructure by:

    a. Working with private-sector entities and non-governmental organizations in focusing on cybersecurity and criminal justice practices;

    b. Striving to align penal codes on an international level in order to simplify law enforcement and fight the migration of criminals and the regional impacts of cybercrimes;

    c. Using the Global Cybersecurity Index (GCI) to match Member States with high and low capacities for cybersecurity development and infrastructure and to serve as a monitoring and evaluation tool for assessing the cybersecurity capacity to states;

    d. Collaborating with the Unsolicited Communications Enforcement Network to inform Member States of anti-spam security measures, as well as best practices to addressing online fraud, malware, phishing, and viruses;

    e. Using the UN Interregional Crime and Justice Research Institute to support the capacity-building of developing nations via disseminating technical information and research as well as initiating and coordinating public-private partnerships;

2. *Encourages* Member States to create a network of educational scholarship programs to increase the capacity for expertise in developing states to combat cybercrime and proper fulfillment of criminal justice through:

    a. The opportunity to provide citizens of developing nations and least-developed countries (LDCs) with the opportunity to study cybersecurity abroad and contribute to the development of their own country of origin upon completion of the program;

    b. Facilitation of a committee comprised of experts in the field which will meet virtually once a year and is responsible for:

        i. Organizing and promoting an online application form targeted towards the application of citizens from developing countries of origin;
        ii. Evaluating students holistically, but mainly based on their interest level, country of origin and its status as either a developing country, country of origin's GCI, experience, education level, and admission exam results;
        iii. Selecting a specific number of students depending on the amount of funding received for that year to be enrolled in the scholarship program;

    c. Financial support with a contract (up to the total cost of tuition) awarded to selected candidates where they are required to work at least 7 years within the cybersecurity workforce of their country of origin or for CAST in order to strengthen criminal justice responses;

3. *Encourages* Member States, private-public entities, and international agencies, such as the International Criminal Police Organization, to provide financial and technical support of the development of programs that seek to prevent cybercrime in developing nations, with particular attention to:

a. Public programs that educate people on best practices in Internet use, basic computer science skills, and cybersecurity through, but not limited to, community centers, libraries, public schools, and non-profit organizations;

b. Higher education programs devoted to computer science and cybersecurity;

c. Technical training programs outside of higher education focused on computer science and cybersecurity;

d. Internships, apprenticeships, and professional networking programs aimed at law enforcement and law professionals in the private and public sector, such as lawyers and judges;

e. Employment opportunities for citizens with computer science skills such as in the private or governmental sector or by supporting startups in the cybersecurity sector;

4. *Calls for* Member States to establish monitoring and evaluation processes that focus on the progress in criminal justice actions in regard to cybercrimes, the development of national and regional cybersecurity programs, and the level of international emigration of skilled persons after the implementation of the aforementioned policies in developing nations;

5. *Further emphasizes* the importance of proper distribution of burden-sharing within criminal justice responses to cybercrime, as well as technical assistance in the prevention, awareness and research of cybercrime which will enable improved criminal justice responses.

National Model United Nations • NY

Code: CCPCJ/1/2
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrime in All Its Forms

---

The Commission on Crime Prevention and Criminal Justice,

Guided by the principles stipulated by the *Charter of the United Nations* (1945), in which Article 1 and Article 3 emphasize the necessity of maintaining international peace and security and solving international problems through international cooperation,

Acknowledging General Assembly resolution 65/230 on "Twelfth United Nations Congress on Crime Prevention and Criminal Justice", which requested the Commission on Crime Prevention and Criminal Justice (CCPCJ) to establish an open-ended intergovernmental expert group meeting to conduct a comprehensive study of cybercrime and criminal justice responses to cybercrime to emphasize the importance of national legislation including the exchange of information on national legislation,

Acknowledging the significant role Member States have in mitigating cybercrime through the implementation of national policies and encouraging international cooperation between states as outlined in CCPCJ resolution 26/4 on "Strengthening international cooperation to combat cybercrime",

Taking into consideration that there is still no universal definition and clear classification of cybercrime,

Recognizing the *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World* (2010) that enabled a supranational cybersecurity platform and international cooperation in terms of best practice sharing of measures against cybercrime in between Member States,

Reaffirming the importance of information sharing as best practices vary across different cultures and regions in order to ensure proper international implementation of cybersecurity policies in Member States,

Acknowledging the importance of international cooperation among national cyber incident response centers which facilitate capacity building of Member States to investigate cybercrime through exchanging innovative and improved research methods as outlined in *Security Council resolution 2341* (2017) on "Protection of critical infrastructure",

Concerned with statistics given by the United Nations Office on Drugs and Crime (UNODC) *Comprehensive Study on Cybercrime* which reveals such problems as ambiguous definition and classification of cybercrime, insufficient technical trainings for prosecutors and judges, and the lack of monitoring and evaluation mechanisms,

Calling attention to the absence of international legislation focused at mitigating and prosecuting cases of cybercrime and encouraging increased international projects, similar to the Global Action for Cybercrime Extended Initiative (2013), focused on assisting nations in their ability to adopt cybersecurity legislation,

Recalling that the *United Nations Convention against Transnational Organized Crime* does not specifically address cybercrime-related issues, and is only applicable in cybercrime cases if the offence involves an organized crime group,

Noting the importance of updating and improving vital cybercrime security measures including UNODC

Global Programme on Cybercrime and Cybercrime Repository in collaboration with the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal,

1. *Encourages* Member States to work alongside UNODC, technical experts, and the Global Programme on Cybercrime on creating or clarifying legal definitions and classifications of cybercrime within national legal frameworks in order to allow for impartial judgements in response to cybercrimes;

2. *Suggests* all Member States draft new legislation particular to new types of cybercrime and adjust existing national laws to criminalize acts of cybercrime, specifically by:

    a. Borrowing successful experience from Member States which are experts on cybersecurity;

    b. Interpreting the existing laws especially when a case involves cybercrime and other kinds of criminal activities;

    c. Appointing a group of experts to analyze cases and address evolving forms of cybercrime;

3. *Urges* Member States to share and update their particular strategies for combating cybercrime and align these in accordance to UNODC's Global Programme on Cybercrime and Cybercrime Repository;

4. *Recommends* the SHERLOC knowledge management portal as offered by the UNODC to categorize crimes related to cyber activity for a more effective utilization of the data provided as follows:

    a. Offences that are most commonly committed including identity theft, credit card fraud, and phishing of online data;

    b. Offences that need enhanced coordination including infringements on integrity and confidentiality, computer and content related offences, and money laundering;

    c. Offences that infringe on the life, physical integrity and personal freedom such as, but not limited to human smuggling, trafficking and child exploitation;

5. *Further recommends* expanding the Cybercrime Repository to effectively establish cyber security through:

    a. Creating a section focusing on implementation methods for Member States to effectively establish cyber security:

        i. That would analyze the differences between national legislations and detect the most effective method;

        ii. That would offer international workshops and forums for law enforcement agencies and judicial officials as offered by certain regional initiatives which will discuss technical assistance and capacity building, reinforce law enforcement, and establish best legislative procedures and practices;

    b. Forming a *Cybercrime Repository Oversight Commission* which will encourage Member States to participate and contribute to the Repository that consists of technical experts from every region;

6. *Invites* Member States to contribute to such databases of legislation, case law and lessons-learned on cybercrime and electronic evidence as *Computer Incident Response Teams and Global Cybersecurity Index* with the collaboration of UNODC to summary the successful cases and analyze the trend of cybercrime so that a mature and useful plan can be made;

7. *Further invites* Member States to share and implement educational and training programs for the purpose of strengthening cybersecurity measures through means including:

    a. Cybersecurity task forces and public authorities cooperating with the European Union Agency for Law Enforcement Cooperation (EUROPOL) and International Criminal Police Organization (INTERPOL);

    b. Collaborating with the Global Programme on Cybercrime;

    c. Encouraging Member States to establish a policy that focuses on legal trainings and seminars for judges and prosecutors with regards to the technicalities of cyber activities and cybercrime;

    d. Providing relevant assistance with the use of technology and media safely in secondary and tertiary educational paths;

8. *Emphasizes* raising people's awareness of adverse effects of cybercrime specifically by:

    a. Cooperating with non-governmental organizations and non-profit organizations to promote the publicity of cybercrime;

    b. Investing in media advertisement on cybercrime and risks taken with the global Internet;

9. *Calls upon* Member States to adjust their governmental objectives through means such as, but not limited to, the creation of a separate governmental task force to prevent, investigate, and combat cybercrime by:

    a. Considering hosting international or regional events for information sharing encompassing workshops and seminars on best practices;

    b. Working in collaboration with Cybercrime Repository Oversight Committee;

    c. Actively monitoring and evaluating cyber activity to ensure no malicious use of information communication technologies.

National Model United Nations • NY

Code: CCPCJ/1/3
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrime in All Its Forms

---

The Commission on Crime Prevention and Criminal Justice,

Fully alarmed by the increase in presence and diversity of malicious cyber-dependent and cyber-related crimes committed in the digital world and their impact on the stability of critical infrastructure of Member States and enterprise as stated in the *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World* of 2010,

Deeply conscious of the *Universal Declaration of Human Rights* of 1948 which guarantees the right of personal security against derogatory treatment in Articles 3, 4, and 5,

Having considered further the work done in the Council of Europe's *Convention on Cybercrime*, also known as the Budapest Convention of November 2001, for the purpose of protecting "society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation",

Recognizing the importance of protecting Member States against new types of cybercrime by encouraging Member States to implement substantive law and actively utilize the broad data on cybercrime laws and lessons learned as outlined in Commission on Crime Prevention and Criminal Justice resolution 26/4 on "Strengthening international cooperation to combat cybercrime",

Acknowledging General Assembly resolution 65/230 on "Twelfth United Nations Congress on the Criminal Prevention and Criminal Justice", in the creation of an open-ended intergovernmental expert group (EGM on Cybercrime), to conduct meetings toward constituting an extensive study on cybercrime and the need for Criminal Justice responses,

Keeping in mind the International Telecommunication Union's (ITU) Global Cybersecurity Agenda which supplies a framework for international cooperation to enhance confidence and security, designed for efficiency, cooperation and collaboration between all relevant partners by building on existing initiatives,

Reaffirming the need the strengthen international, regional and sub-regional cooperation to prevent and prosecute crimes, specifically cybercrime, by enhancing the national capacity of States through technical assistance as stressed by the 2010 *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World,*

Guided by the *2030 Agenda for Sustainable Development* (2015) and the Sustainable Development Goal 16, specifically targets 16.2 and 16.4, in order to create peaceful and inclusive societies, advance crime prevention and criminal justice,

1. *Notes with* appreciation the discussions held by the open-ended intergovernmental expert group (EGM on Cybercrime), which emphasizes the need to further enhance international discussion and cooperation against cybercrime between Member States and the EGM on Cybercrime in the study of cybercrime and measures to strengthen existing national and international legal and other responses, as well as proposing new legislation;

2. *Further recommends* Member States to follow the Global Programme on Cybercrime in order to enhance cooperation to increase efficiency and effectiveness during the investigation, prosecution and adjudication phases of criminal justice responses to all forms of cybercrime by:

    a. Focusing intently on online child exploitation and abuse within a strong legal framework and creating extensive legal measures to prevent and prosecute child exploitation and abuse;

    b. Strengthening national and international communication between Member States' governmental agencies, law enforcement, and the private-sector in order to educate citizens and increase public knowledge of the risks associated with cybercrime;

3. *Requests* Member States to acknowledge the challenges they face in countering the use of information and communications technologies for criminal purposes and advances by analyzing their own vulnerabilities in order to:

    a. Present a yearly report based on the discoveries found in the analysis using the United Nations Office on Drugs and Crime's (UNODC) Global Programme on Cybercrime proposed clustering in the identification of:

        i. Offences against the confidentiality, integrity and availability of computer data and systems;
        ii. Computer-related offences;
        iii. Content-related offences;
        iv. Offences related to infringements of copyright and related rights;

    b. Further develop cyber-investigating units with the purpose to focus on criminal trends as well as investigating methods that will facilitate the coordination needed to increase international understanding of the threats to cyber-infrastructure and identify regular vulnerabilities and adverse scenarios to secure critical infrastructure and faster incident response and;

    c. Encourage an increase in cooperation between Member States' and their pre-established agencies, institutions and new-emerging organizations in order to combat discrepancies in the cyberspace;

4. *Encourages* Members States to consider measures to be implemented at a national level, as suggested in open legal agreements such as the *Convention on Cybercrime of the Council of Europe*, also known as the Budapest Convention on Cybercrime, (CETS No. 135) by:

    a. Actively seeking the guidance of the Council of Europe's T-CY Plenary Committees in:

        i. Creating seminars relating to cyberterrorism and the online exploitation of children to educate the public to generate grassroots momentum toward the ratification of CETS No. 135, and;
        ii. Identifying clauses that are not applicable to non-signatories and work with these states toward improvements leading to their signing;

    b. Forming active and ongoing participation in the Council of Europe's annual Octopus Conference, that will enable more Member States to benefit from the sharing of cybercrime expertise;

5. *Invites* Member States to engage on anti-spam measures with organizations such as the Unsolicited Communications Enforcement Network in order to further strengthen their cybersecurity;

6. *Strongly suggests* Member States work with UNODC and the United Nations Institute for Disarmament Research in drafting new specific legislation to address new various types of cybercrime such as:

    a. Identifying with assistance from the ITU and the Cybercrime Repository, the more extreme forms of cybercrime and their possible repercussions, and barring such methods;

    b. Inclusion of protecting intellectual property and prohibiting illegal access to data from online offenders;

    c. Prohibiting trafficking of persons, online radicalization, and child exploitation;

    d. Illegal use of information technology systems for phishing, hacking, ransomware, and other cyber-attacks;

7. *Calls for* an increase in funding to be given to the UNODC which promotes long-term and sustainable capacity building in the fight against cybercrime, along with offering technical assistance in the prevention, and raising awareness along with the use of data collection, and further allowing the use of Intergovernmental Expert Group professionals to organize and conceptualize cybercrime definitions, key concepts, and specific clarifications for each sovereign nation to utilize in the enforcement of substantive law;

8. *Encourages* an increase in coordination and cooperation among Member States, which will include providing assistance to developing nations in building the capacity of national governments and institutional capabilities, in order to expedite efforts in preventing, detecting, investigating, and prosecuting cybercrimes in all its forms;

9. *Suggests* that Member States implement cybersecurity threat assessment programs that pursue the strategic implementation of anti-cybercrime mechanisms at an operational level, this policy ensures that major criminal threats are tackled with an intelligence-led framework that includes:

    a. Developing Multi-annual Strategic Plans (MASP) by evaluating gathered information from cyber-related incidents in order to define and provide strategic measures to effectively combat each threat;

    b. Formulating Operational Action Plans, which dissect the given MASPs with criteria designations that enable the assignment of a priority mark;

    c. Framing a committee of technical experts to analyze above mentioned plans in order to implement preventive recommendations;

10. *Recommends* Member States to create a coalition of panel of experts to create guidance in the determination of jurisdiction in cyber-criminal cases which involve individuals or non-state actors and Member States and potential extradition processes as to accurately utilize national judicial systems and work on formulation of legal frameworks.

National Model United Nations • NY

Code: CCPCJ/1/4
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrimes

The Commission on Crime Prevention and Criminal Justice,

Guided by Article 1 of the *Universal Declaration of Human Rights* (1948), which states that everyone has the right to life, liberty, security of person in all countries,

Deeply conscious of the sentiment offered in the *Convention on Cybercrime* (Budapest Convention), adopted in 2001, which focuses on creating fluid communication between Member States regarding cybercrime laws, investigative techniques, and international cooperation,

Recalling General Assembly resolution 54/49 (1999) on "Developments in the field of information and telecommunication in the context of international security", which expresses international concern for the potential use of information and communication technologies to compromise the security and stability of Member States,

Acknowledging the efforts of the International Telecommunication Union (ITU) in regard to the recollection, regulation, and examination of critical web violations,

Expressing concern that technological advancements, dependencies on the internet, and the dark net have created new possibilities for criminal activities, in particular the criminal misuse of information technologies, child exploitation, the illegal exchange of drugs, and violation of human integrity,

Emphasizing the need of an international database for technical resources on network breaches to facilitate the identification and amelioration of network vulnerabilities,

Acknowledging the United Nations *Convention on the Rights of the Child* (1989) for its efforts to eliminate all forms of child exploitation,

Further highlighting the Optional Protocol to *The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography* (2000), which specifically required parties to prohibit the sale of children, child prostitution, and child pornography,

Further recognizing the United Nations Office on Drugs and Crime (UNODC) commitment to help developing nations withstand cybercrime and possible cyberattacks on their private sectors and governments by providing greater training to governmental agencies and creating greater public awareness of criminal activity,

Endorsing the study published by UNODC entitled Study on the Effects of New Information Technologies on the Abuse and the Exploitation of Children (2015) which emphasizes the vulnerability of children on information and communications technology (ICT) platforms, especially with the ability to exchange large data files with strangers without supervision,

1. *Calls upon* Member States to recognize that preventative measures must focus on trends such as:

    a. Establishment and implementation of technical and managerial measures for access-control and monitoring of unauthorized access to Information-Centric Networking (ICN) facilities;

b. Physical and technical measures for the protection of ICN facilities from natural disasters and other threats, such as terrorist attacks;

c. Hiring personnel for the secure management of ICN facilities;

d. Establishment and implementation of internal control measures, including emergency plans for the secure management of ICN facilities;

2. *Advises* Member States to utilize collaborative efforts with technical specialists to develop a definition of the dark web and consider incorporating the following as components of their individual national definitions:

a. The portion of the internet that has hidden Internet Protocol addresses, or is un-indexed, and cannot be accessed through conventional search engines;

b. The part of the internet that entails illegal criminal activities in cyberspace, such as but not limited to child sexual exploitation and abuse, drug exchange, smuggling of migrants, as well as the illegal exchange of small arms;

3. *Encourages* Member States to establish a multilateral network of Computer Emergency Response Teams (CERTs) focused on proactive and reactive approaches to cybercrime as a matter of international security by:

a. Holding monthly meetings with CERTs in all other jurisdictions in order to facilitate global cooperation;

b. Framing the creation of physical regional centers across the globe in volunteer Member States with the participation of Member State representatives in order to respond efficiently to cybercrime events;

c. Developing CERTs to include representative cybersecurity experts from respective Member States so as to ensure sufficient Member State oversight;

d. Reporting information gathered on possible threats to cybercrime databases in order to be processed by CERTs worldwide;

4. *Proposes* that the UN Group of Governmental Experts on Cybersecurity to, in order to further research the issues of dark web cybercrime and system security, consider extending its agenda to:

a. Include specifically criminal justice violations on the dark web including but not limited to child sexual exploitation;

b. Consider regular correspondence with CERTs in order to maintain a synergistic network;

c. Conduct research into international encryption techniques, like quantum key encryption which Member States can use at their discretion to better protect sensitive documents, the dark web to monitor and document trends in black market activity in the areas of small arms trade, child exploitation, human trafficking, and extremism activity;

5. *Further encourages* Member States to consider the creation of an integrated and coordinated database of information, in collaboration with the UNODC, to aid in responses to cybercrime by:

6.

a. Connecting the aforementioned database to the international CERT network such that information that proves critical to the resolution of adverse cybersecurity events may be collated and utilized by future CERT efforts;

b. Making information available to governments in order to catalyze effective updates to national cybersecurity policy and state-level computer networks as a means of improving overall network security;

c. Noting that information shared in this manner is subject to both the information exchange laws of local jurisdictions and the choices of the overseeing representative of the individual CERT center in that jurisdiction;

7. *Requests* each CERT, in particular coordination with the governmental representatives, to utilize a three-tiered approach to information security in order to preserve the sovereignty of each individual nation over its data, by permitting the inclusion of:

    a. Information that is visible only to the State that has submitted it, which may be utilized by CERTs within that State to conduct its cybersecurity operations;

    b. Information that is visible to all state-level and individual actors that coordinate and work with the cybercrime database which can be utilized to facilitate reactive and proactive cybersecurity measures on local, regional, and global levels;

    c. Information that is open to the public, including but not limited to information on network vulnerabilities that have been patched and the results of previous cybersecurity operations;

8. *Urges* Member States to collaborate, following regulations and processes that have been stated in the *Budapest Convention* and in-line with online actions taken by the ITU on the collection of previous, current, and future possible threats by:

    a. Utilizing the aforementioned database in order to keep close track of specific events to detect any and all weaknesses on the web;

    b. Filtering and demarcating, through the multilateral database, cybercrimes such as online child exploitation of all types, online scamming, drug exchange, security breaches, information theft, so as to be cohesive and practical on the usage of information that will be constantly added to the database;

9. *Suggests* Member States to collaborate with the UNODC and the International Criminal Police Organization (INTERPOL) in establishing a virtual task force respond to criminal activity on the dark web, that will:

    a. Focus upon the identification and prosecution of actors committing cybercrimes on the dark web through coordination with national law enforcement;

    b. Be facilitated by the regional centers of INTERPOL for coordination, such as the European Agency for Law Enforcement Cooperation, National Police organization for the Association of Southeast Asian Nations, the African Mechanism for Police Cooperation, Police Community of the Americas, General Secretariat of the Cooperation Council for the Arab States of the Gulf, and the Arab Interior Ministers' Council;

10. *Recommends* that Member States consider implementing the following national policies as a means to address the development of additional governmental operations in institutions of national security to prevent hacking attacks:

    a. Specialized units within the police, military, and national customs designed to further address potential cyber threats in regard to child sexual exploitation and abuse, drug exchange, smuggling of migrants, as well as small arms and light weapons trade or weapons smuggling;

b. The integration of new Information Technology equipment and specialized software for national police and prosecution to efficiently detect cyber threats.

National Model United Nations • NY

Code: CCPCJ/1/5
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrime in All Its Forms

---

The Commission on Crime Prevention and Criminal Justice,

Reaffirming the principles of sovereignty outlined in Article 2 of the *Charter of the United Nations* (1945), with specific regard to the respect that should be given to national sovereignty and the principle of non-interference in the domestic jurisdiction of Member States,

Guided by the Commission on Crime Prevention and Criminal Justice (CCPCJ) resolution 26/4 on "Strengthening International Cooperation to Combat Cybercrime", which conducts a comprehensive study and responses of Member States on the exchange of information on national legislations, best practices, technical assistance and international cooperation,

Recalling the General Assembly resolution 64/211 on "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" in technical and legislative assistance in countering cybercrime and cyber-terrorism,

Expressing appreciation for the ongoing efforts of Member States to promote the rule of law and strengthen crime prevention and criminal justice, including training criminal justice sectors on combating cybercrime as seen in General Assembly resolution 57/293 on "Programme budget for the biennium 2002–2003" to create a global culture of cyber security,

Further recalling the 2015 *Doha Declaration on Integrating Crime Prevention and Criminal Justice* in addressing the economic and social challenges to all Member States in conducting a study of the problem,

Reiterating the recommendations from the CCPCJ on exchanging information on national legislation, technical assistance, and international cooperation in strengthening existing responses and propose new national international legal responses to cybercrime, as laid out in Economic and Social Council resolution 1992/22 on "Implementation of General Assembly resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice",

Reaffirming that developing nation are in need of funding to create more sound cybersecurity infrastructure based on the United Nations (UN) Development Programme for Developing Nations Conference,

Convinced of the importance of the instruction of new experts and trained governmental agents, who will, in turn, provide adequate and different solutions at the state level in fighting cybercrime, referencing the General Assembly resolution 73/27 on "Developments in the field of information and telecommunications in the context of international security",

Expecting efficient and effective long-term responses to cybercrime, including national coordination, data collection, and effective legal frameworks, as called for in the UN System Chief Executive Board for Coordination's Annual Overview Report of 2014,

Welcoming Member States from the International Telecommunications Union (ITU) with strong IT control environments to provide infrastructure and development along with further accessibility to the internet in developing countries, with acknowledgement to ITU's resolution 136 on "the use of

telecommunications/ICTs for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief",

Aware of the need to prevent cybercrimes through strengthened institutions to centralize their information through an international system as outlined in the UN Global Pulse report on Big Data for Sustainable Development,

Recalling the lack of technological advancements in many Member States due to the lack of monetary support, as noted in the High-Level Committee's Programme Report of the 24th Session,

1. *Calls for* Member States to collaborate with the Global Programme on Cybercrime to promote private-sector engagement in the hopes of protecting the private sector through:

    a. Assisting Member States in recognizing cyber offenses for a criminal justice response in the private sector, such as:

        i. Offenses against confidentiality, integrity, and availability of computer data and systems;
        ii. Computer-related offenses;
        iii. Content-related offenses;
        iv. Offenses related to infringements of copyright and related rights;

    b. Ensuring that all private firms, regardless of size and magnitude, have access to the Global Programme on Cybercrime;

    c. Encouraging collaboration with other Member States, CCPCJ, United Nation Office on Drugs and Crime, and private-sector stakeholders to host national and international information-sharing events, such as conferences and workshops, to promote the collaboration between the private sector and Member States to educate enterprises in criminal justice responses to cybercrime in the financial sector;

2. *Encourages* Member States to work in coordination with other UN entities and agencies to address internal issues regarding the gap between cybercrime and domestic legal systems, such as, but not limited to:

    a. International Criminal Police Organization for further investigations;

    b. ITU to strengthen cybersecurity and receive technical assistance;

    c. Open ended-intergovernmental Expert Group on Cybercrime to better understand the problem between cybercrime and criminal justice responses to Member States, international community members, and the private sector;

3. *Recommends* Member States to establish legal training programs and seminars for judges and prosecutors that focuses on the technicalities of financial cyber activities and cross-border cybercrime criminal justice by determining the financial cybercrime and technicalities, such as fraud, phishing, cross-border economic hacking, and spreading hate and inciting terrorism:

4. Specifying the punishments that will be given to the offender concerning years of imprisonment and the penalty fee;

5. *Expresses* its hope for the creation of an international "sovereign cloud", with the cooperation of domestic law enforcement which secures data by giving all public institutions the option to centralize their information through a secure system, resulting in data that is less susceptible to theft by global criminal organizations, thus minimizing cybercrime through preemptively combating the issue of financially and informational motivated attacks;

6. *Further invites* Member States to collaborate with international financial institutions, such as the International Monetary Fund (IMF), to contribute to technological advances following inclusion of all nations to tighten cybercrime loopholes through special drawing rights within IMF by:

    a. Encrypting data protection, privacy, and cybersecurity;

    b. Contacting developed nations to aid nation in need through enhanced infrastructure to help grow an IT control environment to promote a safer cyber environment;

    c. Establishing of a minimum international standard that all nations out to follow to ensure a median of technological involvement and security checks;

7. *Suggests* Member States amend current policies that impose socio-economic-political barriers that impede on Member States ability to have the economic ability to ensure the safety of financial sectors, private enterprises, and technological development from cybercrime related attacks.

National Model United Nations • NY

Code: CCPCJ/1/6
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Criminal Justice Responses to Cybercrime in All Its Forms

---

The Commission on Crime Prevention and Criminal Justice,

Affirming its commitment to the *2030 Agenda on Sustainable Development*, particularly Sustainable Development Goal 16 in its effort to strengthen relevant institutions by combating inter alia cybercrime in all its forms,

Mindful of the importance of raising awareness of cyber-related crimes and educating the public as a means of combating cybercrime,

Recognizing the need for cooperation between States and the private sector in combating cybercrime and to protect legitimate interests in the use and development of information technologies,

Strongly emphasizing the support of international information sharing to effectively share best practices and information to establish joint research as well as enhanced international communication regarding the exchange of information between law enforcement entities,

Acknowledging the work of the International Telecommunications Union (ITU), which emphasizes cooperation and consensus between Member States and the private sector on all aspects of information and communication technologies (ICTs),

Endorsing the 2007 Global Cybersecurity Agenda launched by ITU, which is committed to enhancing security measures in the information society by encouraging collaboration and information sharing between Member States,

Keeping in mind that in the 2010 Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, Member States noted that the development of ICTs and the increasing use of the Internet created new opportunities for offenders and facilitated the growth of crime,

Reaffirming General Assembly resolution 73/218 on “Information and communications technologies for sustainable development” concerning the need to implement safeguards of Critical Information Infrastructures (CII) to ensure global cybersecurity,

Welcoming also the efforts of the Human Rights Council resolution 34/7 on “The right to privacy in the digital age” to secure privacy rights of citizens and prevent victimization from perpetrators of cybercrime,

Referring to CCPCJ resolution 26/4 on “Strengthening international cooperation to combat cybercrime”, which stresses the urgency of strengthening international cooperation to provide legal and practical exchange of information with the international community,

Deeply conscious of the sentiment offered within the Council of Europe’s 2001 Budapest Convention on Cybercrime, which focuses on creating effective communication between Member States regarding cybercrime laws, investigative techniques, and overall cooperation,

Recalling the Global Programme on Cybercrime and its efforts to build Member State capacity to address malware and ransomware, particularly through strengthened national and international communication in order to improve knowledge of cybercrime within the public and private sector,

1. Encourages all Member States to work in cooperation with officials from the ITU and Global Programme on Cybercrime to increase awareness of the growing dangers by facilitating trainings for the public such as:

    a. Workshops and training that are available to all citizens to increase the knowledge of the risks of cyberspace and to be able to troubleshoot cybersphere breaches;

    b. Seminars targeted at training government officials in recognizing weaknesses in cyber infrastructure and the potential consequences thereof, as well as proper cyber etiquette that ensures safety from cyber espionage and attacks;

2. *Calls upon* Member States to develop programs that address the laws, challenges, and experience of international CIIs by fostering information sharing of cybercrime data with Member States which may be utilized to:

    a. Develop national cybersecurity policies which underscore the importance of CIIs for nations and identify potential risks;

    b. Implement CII Protection Programs which emphasize robust and systematic cyber risk management processes across all levels of CII organizations;

    c. Facilitate multilateral partnerships between Member States to increase knowledge by sharing on best practices regarding the implementation and enforcement of effective legislation such as the Association of Southeast Asian Nations' Cyber Capacity Development Project;

3. *Recommends* Member States adhere by the guidelines of the Global Program on Cybercrime to develop national and local action plans based upon data received through collaborative training exercises and implement safeguards against imminent threats and pressing environmental factors such as malware and ransomware attacks on ICTs by:

    a. Collecting and cataloging data for scientific research and possible adaptations to the legislative framework for prevention of further crimes and investigations;

    b. Administering cybercrime research workshops among the public sector that coordinate combating cybercrime by training task forces and public authorities to improve responses to cybercrime on a national basis;

4. *Considers* Member States to foster multilateral partnerships with non-governmental agencies such as the International Criminal Police Organization to provide thorough technical training for law enforcement officials in responding and investigating cybercrime by:

    a. Working alongside the United Nations Office on Drugs and Crime in facilitating the process of exchanging ideas and discussing current trends of combating cybercrime both internationally and regionally;

    b. Facilitating international conferences, such as Global Cyber Security Summit, in collaboration with CCPCJ and International Telecommunications in order to present, develop and share educational programs to mitigate the risk of cybercrime related-felonies;

    c. Developing enhanced national cyber situational programs with involvement of multi-sector entities in conducting cybersecurity exercises with complex scenarios, such as the European Union Agency for Law Enforcement Cooperation and the Joint Cybercrime Action Taskforce

(J-CAT) exercise which simulated inter alia an arrest and shutdown of an illicit phishing website;

5. *Requests* Member States to involve both the private sector and specialized non-governmental organizations (NGOs) to provide necessary training to raise awareness for cybercrime and the misuse of ICTs by:

    a. Integrating a cybersecurity program focusing on cyber-exploitation in secondary and tertiary systems of the educational systems to exercise skills on combating issues regarding the cybersphere;

    b. Launching workshops and training that are available to all citizens to increase the knowledge of risks of cyberspace and be able to troubleshoot cybersphere breaches;

6. *Calls upon* Member States to involve both the private sector and specialized NGOs to implement educational initiatives regarding cybercrime regarding the misuse of ICTs by:

    a. Integrating cyber proficiency programs focusing on cyber-exploitation in secondary and tertiary systems of the educational systems to exercise skills on combating issues regarding the cybersphere;

    b. Making the public and private sectors knowledgeable of the key principles of cybercrime such as but not limited to the facts that:

        i. Perpetrators can operate outside geographical borders;
        ii. The majority of the internet is hidden from traditional search engines, increasing the difficulty for law enforcement entities to investigate such cases;

7. *Requests* that all Member States prioritize the exchange of relevant information concerning legislation, challenges, and experience to promote cooperation in all aspects of cybercrime by:

    a. Facilitating multilateral partnerships between Member States to increase knowledge sharing on best practices regarding the implementation and enforcement of effective legislation such as the Association of Southeast Asian Nations Cyber Capacity Development Project;

    b. Strengthening initiatives, such as Global Cyber Security Agenda, that strengthen technical policies and establish crisis centers for cybercrime in all Member States;

8. *Advises* Member States to pursue common legislation for cybercrime by adopting appropriate policies that encourage:

    a. Legislation that publicize substantive criminal offenses and declassifies information that is pertinent to inform the public sector on the necessary precautionary measures against certain elements and patterns of cybercrime;

    b. Legislation that will establish international norms and standards that streamline cyber-criminal prosecution processes, especially cybercriminals whose victims are beyond the geographical boundaries of the Member State in which they reside.