NMUN•NY 2021

28 – 31 March 2021

Documentation of the Work of the Committee on Crime Prevention and Criminal Justice (CCPCJ) NMUN Simulation*

Conference A

* National Model United Nations (nmun.org) organizes simulations of the UN. The resolutions in this document were the work of dedicated college and university students attending our conference. They are not official UN documents and their contents are not the actual work of the UN entity simulated.

Committee on Crime Prevention and Criminal Justice (CCPCJ)

Committee Staff

Director	Vikram Sakkia
Assistant Director	Matthias Burtscheidt
Chair	Savannah Sima

Agenda

I. Combating Organized Cybercrime

II. Combating Illicit Organ Trafficking

III. Improving Vulnerable Persons' Access to Justice Including a Fair Trial

Resolutions adopted by the Committee

Code	Topic	Vote
CCPCJ/1/1	Combating Organized Cybercrime	21 votes in favor, 2 against, 3 abstentions
CCPCJ/1/2	Combating Organized Cybercrime	Adopted by Acclamation
CCPCJ/1/3	Combating Organized Cybercrime	14 votes in favor, 8 against, 4 abstentions

Summary Report

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

I. Improving Vulnerable Persons' Access to Justice Including a Fair Trial
II. Combating Organized Cybercrime
III. Combating Illicit Organ Trafficking

The session was attended by representatives of 26 Member States.

On Sunday, the committee adopted the agenda of II, III, I, beginning discussion on the topic of “Combating Organized Cybercrime” By Monday, the Dais received a total of four proposals covering a wide range of sub-topics including: creating an international definition for cybercrime, education against cyber-attacks, and capacity-building to raise awareness and to create protection schemes. The creative spirit of the solutions was evident as new proposals were discussed within the body to combat organized cybercrime.

On Wednesday, three draft resolutions had been approved by the Dais, one of which had two friendly amendments. The committee adopted three resolutions following the voting procedure. The first of which had 21 votes for, 2 against, and 3 abstentions. The second received unanimous support by the body, adopting by acclamation. The final one passed with 14 votes for, 8 against, and 4 abstentions. The resolutions represented a wide range of issues including managing resources affected by the COVID-19 pandemic, monitoring the transfer of cryptocurrency, and establishing a thorough definition of cybercrime. The committee eagerly proceeded to a discussion on the topic of “Combating Illicit Organ Trafficking” before concluding the meeting.

Code: CCPCJ/1/1
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Combating Organized Cybercrime

The Commission on Crime Prevention and Criminal Justice,

Recalling the Sustainable Development Goals (SDGs) 16 and 17 of the 2030 Agenda for Sustainable Development (2015), affirming the need for willing and able nations to assist developing nations in their efforts to fight organized cybercrime,

Acknowledging the 2016 *Comprehensive Study on Cybercrime* by the UN Office on Drugs and Crime (UNODC) noting the lack and need of an international definition on cybercrime,

Recognizing the 2010 *Salvador Declaration on Comprehensive Justice Systems and Their Development in a Changing World* that calls for the establishment of an open-ended intergovernmental expert group to carry thorough investigation on the responses of Member States as well as the private sector,

Guided by General Assembly resolution 65/230 (2011) on "Twelfth United Nations Congress on Crime Prevention and Criminal Justice" that states that the Global Programme on Cybercrime is meant to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance,

Recalling resolution 26/4 (2017) on "Strengthening international cooperation to combat cybercrime" of the Commission on Crime Prevention and Criminal Justice (CCPCJ), which established The Global Programme on Cybercrime, and highlights the increasingly high rates of cybercrime in developing states,

Noting the report by the UNODC *Intensifies Action to Combat Child Sexual Exploitation* (2020) that the COVID-19 pandemic compounds organized cybercrime and has led to a 350% increase in phishing,

Highlighting the success of existing national programs such as the United Kingdom's Get Safe Online, an online site that serves as the leading awareness resource and source for help in cyber-related problems, the statistics of such a program can be reported directly to the Global Programme,

Cognizant that higher education programs will help to provide people with knowledge of cybercrime as mentioned by the UNODC in The University Moodle Series,

Deeply concerned that the closure of schools and subsequent movement to virtual learning will increase the trends and threats of child sexual exploitation and abuse as noted in the International Criminal Police Organization (INTERPOL) *Threats and Trends Child Sexual Exploitation and Abuse* (2020),

Keeping in mind the General Assembly resolution 74/247 (2019) on "Countering the use of information and communications technologies for criminal purposes" which establishes an open-ended ad-hoc intergovernmental committee of experts with the aim of specifically countering the use of information and communication technology for cybercrime,

1. *Encourages* the United Nations Economic and Social Council (ECOSOC) to develop a Declaration on the Comprehension of Cybercrime (DCC) in cooperation with private stakeholders and experts in the field, with a focus on:

a. Finding a definition of the phenomenon of cybercrime including a classification of different sources based on the type of activity carried out and rank them according to their severity;

b. Seeking a pathway during the conference to enable more stringent international legislation against cybercrime and universal penalties for cybercrime;

c. Reviewing the DCC by the CCPCJ every three years to ensure it reflects the current technological developments;

2. *Emphasizes* voluntary participation of Member States, private tech companies, and non-governmental organizations (NGOs) to increase collaborative efforts and productivity, with a greater emphasis placed on Member State participation, to assist in improving cooperation between stakeholders of various corporations in the creation of a universal policy on ethical standards;

3. *Recommends* that Member States collaborate with the UNODC to create a framework to strengthen and support the Cybercrime Repository to report instances of cyber-criminal activity in which malware intrusion reports would be given to Member States in aims to:

    a. Assist law enforcement officials in understanding common cybercrime occurs and developing hot spot responses;

    b. Further assist in developing internet and communication technology (ICT) training for law enforcement officials;

    c. Reduce risk by strengthening infrastructure capacities to establish services mitigating massive cyber-attacks;

    d. Offer instances of cybercriminal activity as long as the disclosure would not pose a threat of national security;

4. *Suggests* that all Member States, especially developing states, utilize the resources provided by The Global Programme on Cybercrime to:

    a. Work with law enforcement officials in developing states to create more sophisticated software to combat cybercrime such as utilizing the resources of more developed ICT systems and enabling tracing mechanisms for law enforcement officials to utilize in identifying the local of cyber-offenders;

    b. Set up increased communication between Member States governments and relevant NGOs through annual meetings between regional NGOs and the UNODC;

5. *Invites* Member States to create an institutional education program that includes primary, secondary, tertiary, and general public curriculum, specialized to combat cybercrime and advance awareness around cybersecurity to avoid exploitation and abuse advocating for:

    a. Member States to establish degree programs regarding cybercrime in aims to promoting cybersecurity careers in Member States, ultimately advancing security, and endorsing the utilization of classes such as Information Security, Cyber-Spying, Cyber Terrorism;

    b. Nationwide online educations programs accessible to the general public through local workshops in which online programs would regard online safety, crime identification, and the prevention of the leaking of private data;

c. The education of children and youth on safe usage of the internet in order to make sure no personal information regarding a minor is released online;

6. *Advises* the UNODC Global Programme on Cybercrime to organize annual workshops for Member States regarding prevention, investigation, prosecution, and adjudication of cybercrime by:

    a. Calling upon the INTERPOL to expand their efforts in providing databases and tools in assisting with preparing materials for the Action Plan for Education in Cybercrime;

    b. Promoting workshops and trainings advised to utilize the funds of the UNODC Global Programme on Cybercrime;

    c. Promoting additional capacity building workshops from the UNODC within national frameworks for Member States with growing economies that lack the secure technological infrastructure to successfully combat cybercrime;

7. *Welcomes* all Member States to voluntarily participate in the Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes that will be held in May of 2021.

Code: CCPCJ/1/2
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Combating Organized Cybercrime

The Commission on Crime Prevention and Criminal Justice,

Noting deep concerned that only 15% of law enforcement agencies in developing states have the capacity to effectively combat cybercrime as noted in the Internationals Criminal Police Organization's (INTERPOL) 2019 report *Transnational Organized Cybercrime in African Regions*,

Noting further the fact that private corporations such as those engaged in the Open Cybersecurity Alliance (OCA) have advanced technologies and ideas which can potentially provide great benefits to international cyber security,

Aware that in 2015 the United Nations Office on Drugs and Crime (UNODC) established the cybercrime repository that greatly benefits the general public but acknowledges that a more regional and government-specific cybercrime repository would be useful based on past successes of the Economic and Social Commission for Western Asia (ESCWA) and other similar small, region-based groups,

Taking note of the *International Covenant on Economic, Social, and Cultural Rights* (1966), and Norwegian Institute of International Affairs Report (2015), subsequently stressing the necessity of centralizing and building up the capacity of capable domestic information communication technology infrastructure, and its strengthening as a preventative and proactive measure,

Reiterating the success of existing domestic ad hoc advisory bodies such as the *Cyber Security Experts Association of Nigeria* (CSEAN) which works to raise awareness in regard to information security best practices, as well as holding healthy debates to expand the audiences' knowledge, awareness and understanding of the issues around cybercrime,

Bearing in mind General Assembly resolution 74/247 (2019) on "Countering the Use of Information and Communications Technologies for Criminal Purposes," to provide a framework for the implementation of intergovernmental ad hoc advisory bodies such as the UN Intergovernmental Expert Group on Cybercrime (IEG),

Acknowledging the use of Sharing Electronic Resources and Laws on Crime (SHERLOC) platform as a best practices database for strategies on a regional and international level and noting the use of SHERLOC as a promoted program by the United Nations Convention against Transnational Organized Crime (UNTOC),

Recognizing the effective contribution of non-governmental organizations (NGOs) involved in cybercrime such as Interpol Global Complex for Innovation (IGCI) towards supporting the provision of development facilities,

Guided by the call of the International Committee of the Red Cross (ICRC) for governments to protect healthcare facilities from cyber operations, noting the conclusions from the Journal of Medical Internet Research study Cybersecurity in Hospitals: A Systematic, Organizational Perspective (2018) of the necessity of legislation,

Fully aware of the success of initiatives such as *African Cyber Risk Institute*, which is a regional, cross sectoral capacity building campaigns that provides a platform for the public and private sectors within the African region to easily collaborate, identify existing gaps in the regional cyber security response, and provide the resources necessary to best combat organized cybercrime within the region,

Fully alarmed by the fact that the aggregate value of cryptocurrency is almost $214 Billion, and that cryptocurrencies are frequently criticized due to their exchange rate vulnerabilities as well as their frequent use in illegal activities and exchanges, as explained in the UNODC's report *Darknet Threats to Southeast Asia* (2020),

Deeply concerned by the fact that cybercrime and cyber-enabled crime offers a potential avenue to replace the income lost by organized criminal groups that relied on traditional criminal enterprises that have been constrained by virus-control efforts as stated by the Global Initiative's report *Crime and Contagion: The Impact of a Pandemic on Organized Crime* (2020),

Affirming the *UN Framework for the Immediate Socio-Economic Response to COVID-19* (2020) which specifically outlines the importance of protecting health services and health systems during the crisis,

Noting with concern the recent development by many terrorist organizations in the exchange of cryptocurrencies through social media platforms outlined in letter 2021/68 (2021) from the Chair of the Security Council,

Recalling the effectiveness of the Financial Action Task Force (FATF) with cryptocurrency exchanges as outlined in the Financial Action Task Force's 2016 report *Consolidated FATF Strategy on Combating Terrorist Financing*,

Taking note of INTERPOL's *Digital Security Challenge* which is a public-private partnership that utilizes simulated investigations and virtual training sessions to develop law enforcement agencies response capacity for various facets of cybercrime including but not malware attacks, ransomware attacks, and various other cybercrime threats,

1. *Calls upon* further development of open-source software (OSS) through cooperation with the United Nations Development Programme Global Centre for Technology, Innovation, and Sustainable Development (UNDP) and OSS-active organizations in order to respond to the shifts in the cybersecurity landscape and integrate cybersecurity products aimed at both preventing and post-managing organized cyber-attacks by:

    a. Inviting Open-Source Initiative (OSI) approved licensing on the source codes of open-source cybersecurity tools in order to ensure stable supply, co-development, and transparent usage;

    b. Encouraging developing nations to apply open-source cybersecurity tools on both the private and state level and conducting their own updates and technological advancements through utilizing such software that has been distributed;

    c. Recommending Member States to voluntarily collaborate with cybersecurity product developers joined in the OCA in order to develop interoperable anti-virus scanners;

    d. Suggesting OSS to strengthen firewall and defense capacity against security breaches of healthcare facilities in consideration of the COVID-19 pandemic;

2. *Emphasize* the need for strengthening of the capacity of domestic infrastructure, including but not limited to healthcare and resource facilities, to ensure protective, preventative, proactive, and thereafter measures by:

    a. Encouraging nationwide installations of technical equipment such as deep packet inspection (DPI) tools onto internet service providers (ISP's) by the nation state, thus warranting for the inspection of data to ensure the protection of firewalls in real-time; monitoring of data allowing for information exchange through public sector facilities;

advocating for the centralization of national public communication networks in order to counteract potential threats;

b. Suggesting the utilization and implementation of voluntary ad hoc intergovernmental committee of experts such as the IEG to advise proper procedures in the potential event of incident concerning cybercrime;

c. Emphasizing the use of a secure network and database to provide information relating to how to repair the effects of a cyber-attack on governmental infrastructure and how to properly defend from them;

d. Utilizing SHERLOC as a secure database for cybersecurity as agreed by a multilateral agreement to securely share information pertaining to the cyber-attack and protect sensitive information from the attack;

e. Advising the use of simulated attacks to prepare infrastructural pieces for cyber-attacks and cyber terrorism by the Member State that is simulating the attack to protect their secure data which could be conducted by use of inactive governmental infrastructure;

f. Encouraging Member States to participate with NGOs reaffirming the support of IGCI to provide voluntary scamming training education-based capacity-building to members of the Criminal Justice Department Offices within Member States' borders, as well as training of government administrators by the state in preservation of information relating to cyber-attacks;

g. Proposing the implementation of state legislation to ensure the protection of critical healthcare networks and essential medical services, permitting each Member State to define what constitutes such networks and services, regarding the targeted use of cybercrime and cyberattacks on such infrastructures;

3. *Promotes* the adaptation of a regional cybercrime repository, maintained by the UNODC, based on the already-existing cybercrime repository with the purpose and function of:

    a. Assuring that Member States can maintain their sovereignty and sensitive information yet still have access to the benefits of the repository by not requiring any type of information contribution or sharing of explicit details;

    b. Reducing the probability of similar cybercrimes occurring in nearby Member States by making pertinent information readily available to those within the region;

    c. Outlining the various problems of specific cybercrimes and solutions to such by suggesting the voluntary contribution of information, as indistinct or as detailed as the Member States sees fit;

    d. Categorizing the types of cybercrime, including but not limited to, information sought, infrastructure attacked, possible preventative and responsive measures, subsequently measuring their effectiveness, and possible additional resources;

4. *Encourages* the voluntary regional collaboration and intelligence sharing between governments and private enterprises and NGOs by creating a two-way benefit system, operating on an opt-in basis, which will function by:

    a. Collaborating to conduct extensive research initiatives which can be used to identify gaps in responses and challenges specific to the region and utilize this information to

create recommendations, toolkits, awareness training and workshops and other relevant capacity building mechanisms;

b. Providing a trusted set of resources that can be utilized by governmental bodies, businesses, civil society actors, and the public sector to identify emerging threats to information and information systems and use this data to formulate more effective response strategies;

5. *Consider* the adoption of voluntary regulation, by the Member State, on transferring of cryptocurrencies to a fiat currency to be withdrawals by banks to better mitigate monetary fraud and laundering and illegal purchases by:

    a. Having only national banks be able to trade with cryptocurrencies;

    b. Regulating the transferring of cryptocurrencies to bank accounts to prevent the conversion of a cryptocurrency into fiat money, it could potentially devalue the use of the currency and limit transactions.

Code: CCPCJ/1/3
Committee: Commission on Crime Prevention and Criminal Justice
Topic: Combating Organized Cybercrime

The Commission on Crime Prevention and Criminal Justice,

Acknowledging that the UNODC *Comprehensive Study on Cybercrime* (2016) concluded that only 1% of cybercrimes have been reported to the police and that cybercrime is very difficult to solve without outside resources, and noting the severe lack of specialized officers equipped to combat cybercrime with only 20% of special officers having advanced information technology training,

Expressing its appreciation of the East African Communications Organization (EACO) and its efforts to give everyone in the East African region access to communication, as reported by the EACO,

Supporting the work done by Computer Incident Response Teams (CIRT) established in Member States to study internet security, discover vulnerabilities, and provide security-related assistance to communities to contribute to combating cybercrime,

Viewing with appreciation the bilateral workings of the UNODC Terrorism Prevention Branch, which engaged in specialized three-day training programs on strengthening the capacity of law enforcement to combat the financing of organized cybercrime groups using cryptocurrencies,

Further noting over 90% of Member States put in place specialized structures for the investigation of Cybercrime as stated by the 2016 *Comprehensive Study on Cybercrime*,

Deeply concerned about the rise in cybercriminal activity in the international scope of our communities in the wake of the COVID-19 pandemic,

Expresses its hope for further cooperation through regional agreements through national frameworks such as the 2007 *Cairo Declaration against Cybercrime*, a set of policy recommendations and guidelines developed from the first regional conference on cybercrime held in Cairo on 26/27 November 2007,

Approves programs such as the *Cybercrime Contact Center (CCC)* Initiative working towards increasing public-private partnerships (PPPs) in the attainment of Sustainable Development Goal (SDG) 17.17,

Taking into account that social conditions are relying more than ever on computer networks to interact, work, and shop as more risks are related to organized crime infiltration into the legal economy as of 2020, according to the *United Nations Interregional Crime and Justice Research Institute*,

Recalling the urgency to educate all citizens in the dangers and unfamiliarity of cybercrime as means of prevention, according to the *COVID-19 and its Implications for Protecting Children Online report* (2020) by UNODC,

Welcoming the effort of the UNODC in preparing the newly finalized Global Programme on Cybercrime to provide technical assistance and capacity-building on cybercrime,

Emphasizing the 2016 Joint Action Plan, created by the International Criminal Police Organization (INTERPOL) alongside UNODC, to promote a transnational partnership to fight organized cybercrime,

Approving the collaboration between the International Telecommunications Union (ITU) and Child Online Protection (COP) program, they updated their 2020 guidelines to protect children in cyberspace,

Encourages the developing countries to participate in the Global Programme on Cybercrime, designed by the General Assembly and CCPCJ, to increase efficiency and effectiveness in the investigation, prosecution, and adjudication of cybercrime,

1. *Suggests* Member States to enhance regional bodies through the potential utilization of stakeholders in the communication sector to work with intergovernmental panels by applying the incentivizing public-private structure of the EACO, which coordinates the development of the communications sector through harmonization of policy by taking into account industry innovations:

    a. Devising ways and means to achieve fast, reliable, secure, affordable, and efficient communication services between governments and private entities;

    b. Promoting the development of broadcasting, postal, and telecommunications information and communication technology (ICT);

    c. Help harmonize ICT policy and regulatory frameworks in the Member States;

2. *Recommends* developing Member States to formulate special cybercrime task forces by utilizing the organizational structure of CIRT, which is a department within every federal organization formed to study Internet security, discover vulnerabilities, and provide security-related assistance to communities, the purpose of which would be to:

    a. Facilitate the centralized reporting of incidents;

    b. Perform training and raise the security awareness of users;

    c. Analyze the various logs of both the network devices and the systems logs and intrusion detectors;

3. *Suggests* the adoption of national speed dial numbers specifically for reporting cybercrime-related incidents to help streamline national reporting;

4. *Recommends* updating police hotlines and national broadcasting systems for cybercrime reporting and voluntary national tracking by engaging with the United Nations Economic and Social Council Partnership Forum and United Nations Department of Economic and Social Affairs to use funding streams towards technical training over software and data logging efforts within Member States' law enforcement systems;

5. *Encourages* Member States to support the development of digital software and infrastructure capacity of existing national cybersecurity reporting applications wherein the programs will:

    a. Be overseen by Member States' individual CIRTs or similar programs;

    b. Provide default drop-down options before reporting to solve basic cyber-issues;

    c. Enable access to users with updated information on cybercrimes specific to COVID-19, such as phishing scams related to vaccines and appointments;

6. *Recommends* the International Criminal Court (ICC) to:

a. Adopt a policy to apply broad legislation to criminalize the improper use of informational networks and private networks which can enforce a broad measure against cyberterrorism and cybercriminal outfits;

b. Adopt the policy by the ICC to criminalize the breaching of security and encryption systems within cyberspace to protect federal structures within Member States;

c. Recommend the use of biannual training for staff members of the ICC relating to good internet practices and cybersecurity under the purview of the United Nations Institute for Training and Research;

d. Suggest the practice of annual briefings on major global cybercrime incidents and analysis of how they might fall under the purview of existing international law through the ICC's Diplomatic Briefings;

7. *Suggests* the increase of regional cooperation through the UNODC and such programs as the ITU COP program 2020:

    a. Recommends an annual event to specifically train public officials and teachers so they can spread the international knowledge to prevent cybercrime towards children and civil servants;

    b. Advocates national awareness programs targeting children to spread the knowledge generated through these experts to the vulnerable to protect them as best as possible;

8. *Further suggests* participation in the UNODC fund for training programs having the universal Member States involved, to equip each country with the necessary capabilities to combat and prevent such crime, designed to such ways but not limited to:

    a. Recommending the implementation of training programs for public officials led by the UNODC and other international agencies with a focus on educating the public to the dangers of cybercrime;

    b. Development of newer, sophisticated tools to keep data more secure, funds be donated to and distributed by the UNODC;

9. *Encourages* the Member States to collaborate with regional and international agencies to aid in the implementation of cybercrime training, facilitating coordinated operations and partnerships since collaboration between states and sharing resources are the keys to combating cyber-crime such as:

    a. Continually working with existing programs such as but not limited to International Criminal Investigative Training Assistance Program (ICITAP), Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and INTERPOL facilitating cooperation between states because they own and operate 85% of all critical infrastructures;

    b. Developing professional and transparent law enforcement institutions in each Member State;

    c. Increasing coordination and cybersecurity capabilities, allowing for better communications to investigate crimes and catch criminals;

    d. Training for border officials on patrolling procedures and surveillance techniques, early warning signs, technical advice, and assistance.