**FORUM:** Commission on Crime Prevention and Criminal Justice

**QUESTION OF:** Measures to Counter Cybercrime

**SUBMITTED BY:** South Korea

COMMISSION ON CRIME AND PREVENTION AND CRIMINAL JUSTICE,

*Recognizes* the UNODC as a UN organization that will further have the intentions of preventing and halting cybercrime globally, as it is currently using its resources in order to protect governments private data and tracking any major cybercrime attacks,

*Defines* cybercrime as any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them, or, in a broader sense, as any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offerings, or distributing of information by means of a computer system or network,

*Noting* a new report which has put a number worldwide cybercrime costing an estimated $600 billion USD a year within foreign and domestic fraud and cybercrime,

*Recognizing* the ITU (International Telecommunications Union) as a UN specialized group that promotes the harmonization of technical standards for information and telecommunications technologies further fostering international cooperation to improve cybersecurity through its Global Cybersecurity Agenda,

*Appalled* that cyber violence against women and girls is an increasing concern additionally despite the lack of data estimations are showing that one in ten women have experienced some form of cyber violence since the age of 15,

*Recalling* resolution 65/230 debated during the Twelfth United Nations Congress on Crime Prevention and Criminal Justice committee and covers various cybercrime and international cybersecurity issues and their connecting solutions,

*Noting* that cybercrime and fraud scale revealed in annual figures that there were an estimated 3.6 million cases of fraud and two million computer misuse offenses in a year,

*Recognizing* the Salvador Declaration as the 12th United Nations Congress on Crime Prevention and Criminal Justice that calls for the Member States to adopt the ideas surrounding their criminal justice systems to prevent further cybercrime,

1. Recommends that all member states ratify and implement Resolution 65/230 as it was previously created in order to add transparency and for the prevention of cybercrime, along with the use of the Salvador Declaration which further calls for the unification of member states to fight cybercrime and the implementation of proper methods and strategies with the direct intention of preventing cybercrime;
2. Wishes for the allocation of financial resources to develop to UNODC by implement effective policies, programs and training that directly deal with crime prevention, criminal justice and the prevention of cybercrime, further providing the UNODC with a level of resources necessary and collaborations of member states to implement successful strategies to combat misuse of the internet and prevent further cybercrime;
3. Asks for the implementation of new globalized schooling programs to be overseen by the UNODC, which will teach young adults about the detrimental consequences of cybercrime and how protecting and securing private data is of the utmost importance in relation to privacy and exploitation through cybercrime by means such as but not limited to:
   1. classes taught within schools or external classes which will have the intention of teaching:
      1. young adults the importance of privacy and network security while in use of social media or other network pieces
      2. the promotion and support of preventing child sexual abuse and exploitation through the internet
   2. classes should be taught from ages 9-24 as today’s digitial age means that much younger children are online and at risk of being the victim of cyber-crime and must be taught the necessity of internet privacy,
   3. for countries that are unable to directly implement programs funded through the United Nations Development Programme (UNDP) or World Bank (WB) based on evaluations of a nation’s:
      1. political or economical instabilities within the government
      2. unemployment rates throughout designated regions
      3. GDP per Capita;
4. Asks for the implementation of online programs aimed to raise awareness of cybercrime in the private sector and provide businesses the necessary resources in order to establish proper cyber security protocols, while also encouraging investment by the private sector for business operations, risk management and innovation regarding cybersecurity;
5. Requests for the creation of the UNCCPF (United Nations Cyber Crime Police Force) with the intentions to efficiently and effectively respond to cybercrime, including international coordination between member states governments, data collection and legal framework that can be used to further track and arrest any individuals or groups that may be using cybercrime as a method to destabilize or cripple:
   1. member states government
   2. domestic companies
   3. or any other deemable group that may be vulnerable to cybercrime;
6. Recommends the further implementations and use of International Telecommunications Union (ITU) in order to combat cybercrime and implement stronger and more effective cybersecurity within governments in order to reduce and diminish the effectiveness of cybercrime, with the intentions of:
   1. implementing programs and training exercises to further inform individuals about the struggles consequences of cybercrime
   2. and communicating between member states in order to ensure cybercrime attacks and data relating to said attacks, are tracked and notified to the UNCCPF or UNODC to further reduce cybercrime attacks;
7. Calls for biannual meetings between member states and relevant UN groups such as UNCCPF, UNODC, ITU, in order to confirm that governments’ critical data or privacy are not vulnerable to any cybercrime attacks, while furthermore discussing information in regards of:
   1. measures to implement teaching programs previously stated and any progress that may have been made
   2. collaboration and cooperation between participating member states and UN parties such as UNODC or UNCCPF are efficient and effective in discussing further intentions and methods to further develop strategies to combat cybercrime;
8. Further asks for the UNCCPF and ITU to create optional protective cybersecurity systems and training programs in order to secure any data or information that could be stolen and used against member states, further decreasing the chances of cybercrime within nations:
   1. funding for protective systems and programs to be funded by World Bank if member state feels they are unable to implement proper cybersecurity protection
   2. training for programs to be overseen by UCCPF and consists of several exercises and effective teaching styles that are best suited to teach individuals information in regards to cybercrime;
9. Calls for the UNODC to implement more efficient and effective protections that will have the ability to reduce and minimize fraud on a global level by means of but not limited to:
   1. implementation of additional security sites that are added on to willing online retailers or banking companies that may reduce and stop fraudulent banking
   2. additional measures to combat identity theft which has been affecting many unsuspecting individuals of various ages, through strategies such as but not limited to:
      1. implementing extra protective steps on all transactions to further verify individuals making purchases
      2. additionally tracking and detecting of extreme purchases that are out of the norm and contacting the user to confirm that purchases are in fact viable,
   3. enacting law to force web companies to periodically simulate sophisticated attacks against computer hardwares and softwares to ensure that responses are valid and timely;
10. Designates the UNCCPF and ITU with monitoring major cyber markets under the dark web with the aim of collecting data and tracking down producers and the distribution of illegal products along with malware, which may be used improperly or undermining specific companies’ legal obligations;
11. Further requests for the creation of the Online Consumer Protection Organization (OCPO) that would collaborate with major Online Service Providers (OSP’s) like Google, Amazon, Facebook, Apple (GAFA) in order to encourage efficient security measures at the consumer level, including but not limited to:
    1. symbol variety in a password/passphrase
    2. two-factor authentication;
12. Encourages for the establishment of a UNODC-synthesized guideline that would serve as a basis for anti-viruses as well as protective and responsive cyber-architectures (firewalls, DRP’s, session protections) to come, this guideline would be implemented (failure to implement would result in the shutdown of that referenced platform) by large platforms defined by:
    1. their capacity to hold multiple user connections
    2. their capacity to perform rapid data transactions
    3. The number of daily active users;
13. Requests companies that possess Critical Information Infrastructures (CIIs) to be held accountable for keeping their CII secure with appropriate protective cyber-architectures that meet the standards established in clause 12, with the intention of erasing vulnerabilities in the private sector by standardizing all protection of critical data;
14. Wishes for Small and Mid-Sized Businesses (SMB’s) to run an awareness program across their employees as they are the most significant victims of even the simplest phishing attacks, and for these same businesses to use a more secure architecture of access from employee to central data in order to prevent a large scale attack taking origin from a single employee;
15. Requests governments to recommend companies to join some organisation and international cooperation groups in order to eliminate piracy as well as establish an international law in cyberspace, which punishes anyone who commits action of cybercrime;
16. Further requests companies possessing relevant data such as statistics on simulaions and previous cyber attacks to forfeight appropriate information and data to the UNCCPF or governments involved if that data is deemed as beneficial to an investigation on an act of cyber-crime or cyber terrorism.