**FORUM:** Crime Prevention and Criminal Justice

**QUESTION OF:** Measures to ounter Cybercrime

**SUBMITTED BY:** Chile

CRIME PREVENTION AND CRIMINAL JUSTICE,

*Recognizing* the definition of cybercrime stating “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause any physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the internet.”,

*Emphasizing* the need for having not only cooperation within the U.S, Philippines, and Chile but international cooperation and relations to encourage ultimate efficiency when tackling this issue,

*Recalling* that cybercrime can reach a revenue of approximately a total of 1.522 trillion annually, this could be for financial gain, however, this is not the only reason why cybercriminals commit cybercrime. The reason why they might commit cybercrime could be because information warfare, to make a social point, for an intellectual challenge, or for phishing scams,

*Urging* distinction between advanced cybercrime, a specific attack against hardware and software, and cyber-enabled crime, an existing crime that was augmented through the use of the internet,

*Requesting* that cybercrime prevention must be focused in crime hotspots, such as the United States (which produces 33% of the world’s malware), China (which produces 30%) and Brazil (which produces 13.7%),

*Recalling* resolution A/RES/57/239, which declares that local communities comprise of the primary defense against cybercrime and close-knit populations are, on average, less likely to commit join cyberterrorism groups,

*Remembering* resolutions A/RES/56/121 and A/RES/55/63, which claim that while the internet does create space for crime, it moreover stimulates economic growth and education, and thus must remain free of censorship,

*Advocating* the continued work of the UN Group on Cybercrime and Cybersecurity, created by High-Level Committee on Programs to help collaboration and create a global policy on cyber attacks, with a focus on how to ensure cybersecurity remains an instrumental part of the global conversation,

*Understanding* that cybercrime generally stems from monetary needs, either through collecting payment for information gathered by hardware or theft of passwords and private information,

*Encouraging* the Five Eyes, Nine Eyes, and Fourteen Countries Pact to expand to other UN member states,

*Noticing* that 50% of all cyber crimes carried out were performed on online shops, taking details from the victim, which are credit card information, their number and other crucial information that is meant to be hidden. Most importantly is that their identity is stolen, this gives the opportunity that cybercriminals can take the identity of someone else,

*Recognizing* that cybercrime is a low-risk, high return enterprise in which individuals and groups of actors leverage cyberspace for financial gain or other malicious ends,

*Recalling* Chapter II of Punishable acts which states that any data interference or interceptions are under any circumstances a punishable act,

*Welcoming* the efforts made by other nations with laws against cybercrime to promote cooperation, ultimately empowering security within the world,

1. Asks that all countries make cybercrime illegal and a punishable crime internationally, thereby consolidating peace between partners;
2. Calls for a short international report number to report any forms of cybercrime in an emergency. If this number is misused, it will face the same consequences as the emergency number. There is no need to have different numbers depending on the continent due to the fact that most cybercriminals commit crimes internationally;
3. Promotes the need to strictly monitor websites that hold any personal information, to prevent phishing scams and to ensure the safety of the user and cooperating with different websites to secure the cyber security;
4. Encourages states to educate people about the prevention of cybercrime, to minimize the probability of them becoming victims of cybercrime;
5. Expecting that all nations follow chapter II of the Punishable Acts in the Republic act no.10175;
6. Emphasizes that all electronic documents and signatures to be regulated regularly, to prevent them from being taken and used;
7. Supports making Virtual Private Networks (VPNs) accessible to all people, through:
   1. use of international funding, secured by the office of the UN Special Rapporteur on the Right to Privacy, the State parties to the aforementioned ICCPR, and nongovernmental organizations such as Privacy International
   2. augmented accessibility to secure internet servers with Secure Sockets Layers (SSLs)
   3. use of logs with VPNs to stop cybercriminals and ensure justice with a modified Tor system to allow authorized intelligence analysts to access files from heavily encrypted transmit data through government relay servers, shredding past movement to stop hackers from gaining access to logs
   4. promotes country-specific response plans to cyber attack based on Computer Security Incident Response Teams to be subsidized by the UN Office on Drugs and Crime in specific industries, namely:
      1. commercial organizations
      2. service provider customer bases
      3. the financial and energy sectors
      4. local and federal law enforcement agencies;
8. Requires yearly risk assessments undertaken by federal auditors for governments, critical infrastructure, and corporations with significant proportions of economic ties in the international community to limit the average time it took for companies to identify a breach (197 days) and time to contain the threat (69 days);
9. Responds to election system hacking through the Resisting Ubiquitous Schematic System Interference Action (RUSSIA) Act in order to prevent foreign governments or nonstate actors from interfering in political elections by:
   1. Protecting election infrastructure by coupling electronic voting machines with paper ballots and conducting post-election audits by:
      1. maintaining current election policy to ensure sovereignty, a right guaranteed under Article II of the UN Charter
      2. promoting the use of direct-recording electronic (DRE) voting machines with voter-verified paper audit trails (VVPAT)
      3. condemning the use of blockchain voting software because of its vulnerability to hackers and ballot marking devices for not storing voter choices and nonreadable bar codes
   2. Providing awareness measures to local, regional, and state levels of government for signs of meddling;
10. Endorses access to cyber insurance for individuals and small businesses, specifically covering credit card and account numbers, driver’s license numbers, health records, and Social Security numbers in order to provide recovery of compromised data and repair services;
11. Urges to provide free anti-viruses and firewalls to all nations internationally, to encourage the use of cybersecurity software;
12. Devises a comprehensive strategy for strong cyber defenses, this could be achieved by:
    1. recruiting more cybersecurity specialists and thereby creating a cybersecurity team
    2. enhancing national law enforcement efforts to fight against cybercrime;
13. Requests the international ratification of the Convention on the Right To Cyber Security, a comprehensive document functioning as an addition to Article 12 of the Universal Declaration of Human Rights and Article 17, sections 1 and 2 of the International Covenant on Civil and Political Rights (ICCPR), which both define privacy as a human right, with two aims:
    1. Publicize security breaches from corporations modeled after the European Union’s General Data Protection Regulation, allowing consumers to:
       1. freeze credit
       2. limit insider trading
       3. clarify safe servers;
    2. Requiring free, regularly updated anti-virus software to be provided with computer purchases, modeled after regulations proposed by Australia’s Standing Committee on Communications report.