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

**QUESTION OF:** Measures to counter cybercrime

**SUBMITTED BY:** Brazil

THE COMMISSION ON CRIME PREVENTION AND CRIMINAL JUSTICE,

*Fully aware* that state of cybercrime is a serious and widespread concern which affects many countries, according to official sources, the number of cyber attacks grew by 197 percent in 2014, and online banking fraud spiked by 40 percent in 2017,

*Recognizing* that cybercriminals consider the relationship between the benefits of the proceeds of the crime and the risk of the sentence to be discounted very advantageous,

*Recalling* that most computer attacks come from low-income countries with weak security systems,

*Deeply conscious* that the continuous evolution of computer techniques requires an equally rapid updating of the methods of prevention of computer crimes,

*Considering* that technological innovations in the financial field have simplified with the advent of cryptocurrencies the possibility of transforming the results of computer crimes into money,

*Affirming* that cybercrime is often favored by the lack of awareness of ordinary people on the need to protect their data,

*Reminding* Member States that according to a study commissioned by the European Commission’s Information Society and Media about the “Information Society” made in 2007, malicious software caused damages of up to USD 17 billion in 2003 alone,

*Emphasizing* the fact that preventing cybercrime would also prevent safe-heavens for criminals,

1. Invites the continued revision of laws and measures that limit the vulnerability of services exposed to cybercrime, being more transparent about how they are responding to cybercrime and protecting client data by:
   1. Embittering consequences if the crime is committed,
   2. Intensifying the standard security quality of federal computer and banking systems,
   3. Enacting laws to force web companies to periodically simulate sophisticated attacks against computer hardware and software to ensure that responses are valid and timely,
   4. Establishing and implementing laws and policies to eradicate the irrational support that governments give towards these cybercrime victims;
2. Request the Public Service Announcement (PSA) and other infrastructure to improve public education systems for all potential Internet users about the danger from technology that may arise, and implement precautions to protect mobile devices and reduce social network risks by:
   1. Creating co-educational curriculum programs in school designed for various age groups that provide young people with tools and expertise to understand the root causes of cybercrime in their communities,
   2. Raise public awareness of the real damage that cybercrime emerges in the form of:
      1. Radios,
      2. Television,
      3. Billboards,
      4. Social network,
      5. Advertisements,
   3. Educating from the youngest age preventions of such crime, such as, but not limited to:
      1. Favoring the use of a full-service Internet security suite,
      2. Encouraging the use of strong passwords,
      3. Regularly updating software,
      4. Enhancing security of admin login page;
3. Encourages the increase of funding for support services by:
   1. Dedicating financial resources to develop the use of specialized cybercrime policing units,
   2. Increasing inspections of cybercrime channels,
   3. Investing in innovation and research for the dedication and prevention of digital crimes throughout the latest training techniques and proactive investigation into emerging crimes;
4. Calls upon the urgent establishment of global norms among the major industrial and developing countries on issues of national security and cyber economic espionage conducted by their intelligence agencies and military services;
5. Considers the establishment of an efficient online self-reporting system for cybercrime victims to enable public gathering and analysis of cybercrime statistics, in which:
   1. Victims of cybercriminal attacks stand in need of reporting crime and resulting losses more easily and effortlessly,
   2. The central organization should be responsible for coordinating the whole self-reporting system and for initiating investigations and prosecution of
      1. Cybercriminals,
      2. Terrorists,
      3. Hacktivist groups,
   3. The relationship is enhanced between individuals and law enforcement agencies ensuring adequate protection
6. Requests for the establishment of virtual task-forces, such as the World Cyber Cop, to promote better international coordination between interregional law enforcement and governmental cybersecurity agencies through means such as, but not limited to:
   1. Active partnerships, made with Internet Service Providers (ISPs), Internet Security Organizations, and online financial services,
   2. Authorities require the flexibility to include a variety of stakeholders,
   3. Collaboration with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation;
   4. Encouragement and promotion of further adoption of defensive techniques that can rapidly crowdsource threat data;
7. Draws attention to the promotion and easy availability of pornography especially child exploitation which refers to images or films and writings depicting sexually explicit activities involving a child by:
   1. Allowing law enforcement to intervene and get the tools it needs before a child is assaulted,
   2. Increasing penalties for aggravated offenses, such as but not limited to using a carriage service to transmit indecent communication to a person under 16 years of age,
   3. Favoring the purchase of computer software products that monitor and control the child accesses to the Internet;
8. Urges for the United Nations (UN) to hold a legislation due to the limited reach of existing regional legal instruments as there is a necessity at a goblin level to harmonize legislation on cybercrime;
9. Asks the UN to provide sufficient capabilities such as but not limited to reinforcing international cooperation and dialogue to end cybercrime between:
   1. Governments,
   2. The UN,
   3. Regional organisations,
   4. INTERPOL.