

Resolution GA/3/1.1

General Assembly Third Committee

Co-sponsors: Republic of Albania, Commonwealth of the Bahamas, Republic of Belarus, Republic of Benin, Republic of Burundi, Republic of Columbia, Republic of the Comoros, Republic of Côte d'Ivoire, Kingdom of Denmark, Arab Republic of Egypt, Republic of El Salvador, Republic of Estonia, Federal Democratic Republic of Ethiopia, Republic of France, Federal Republic of Germany, Republic of India, State of Israel, Jamaica, Japan, Hashemite Kingdom of Jordan, Republic of Lebanon, Republic of Liberia, Republic of the Niger, Republic of Palau, Republic of South Africa, Saint Kitts and Nevis, Syrian Arab Republic, Republic of Tunisia, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, Bolivarian Republic of Venezuela.

Topic: Countering the use of information and communications technologies for criminal purposes

Emphasizing that the rights of global citizens should be protected and must be a top priority,

Declaring that cybercrime is a global and complex issue that has significantly grown in recent years,

Fully alarmed that developing countries lack the support and funding needed to combat cybercrime and improve their cybersecurity,

Noting with deep concern the need to grow international cooperation through pre-existing treaties,

Acknowledging that most cybercrime occurs transnationally,

Welcoming the stronger involvement of the UN in the prevention of cybercrimes,

Noting with deep concern trends in cybercrime,

Recognizing the lack of awareness and education about the dangers of cybercrimes,

Desiring a safer digital future for all,

Education on Cybercrime

- I. Recommends that all member states that are able to create courses to discuss the impact of cybercrimes and how to stay safe online for all ages;
- Demands the creation of awareness programs in which cyber attack victims would share their experience and advice in order to let others know how to prevent future occurrences;
- 3. Supports the creation of specialized institutions dedicated to the education of individuals on how to protect themselves, exhibit respectful behavior using ICTs, and be able to teach it to others:
- 4. Encourages countries to run campaigns through various online platforms such as social media to raise cyber crime awareness;

Partnership in the UN

- 5. Advises all member states to enforce stricter consequences against cybercriminals;
- 6. Further requests all member states to offer support through a 24/7 cyber crime specialist helpline dedicated to the victims of cybercrime allowing civilians to report and navigate the problem;
- 7. Invites member states to collaborate in UN-meetings to establish a comprehensive definition of cybercrime, suitable punishment and related categories;
- 8. Strongly encourages forming a new committee to debate, discuss and research cybercrimes, also partnering with a second new committee that implements the first committee's decisions:

Global Cooperation

- 9. Directs member states to form an organization to give resources and funding to underdeveloped nations;
- 10. Encourages nations to adopt international laws;
- II. Requests that member states attend conferences so that they can enhance their knowledge of cybercrime and cybersecurity;
- 12. Strongly suggests that member states have equal access to resources through the creation of a global database;
- 13. Advises countries to sign international treaties to prevent cybercrime that satisfy the needs of all member states:

Protection and Security Against Cybercrime

14. Encourages all member states to host and attend annual summits regarding cyber safety;

- 15. Recommends member states to bring awareness to the use of Al and ICTs for malicious intent;
- 16. Further recommends financial aid be given to underprivileged countries for the use of combating cybercrime, pre and post cyberattacks;
- 17. Advises improvement of security systems globally by partnering with tech companies and manufacturers.