Resolution GA/3/1.1

General Assembly Third Committee

Co-sponsors: People's Democratic Republic of Algeria, Commonwealth of Australia, Republic of Austria, Federative Republic of Brazil, Republic of Cabo Verde, Central African Republic, Republic of Chile, People's Republic of China, Republic of Coôte d'Ivoire, Islamic Republic of the Gambia, Georgia, Hellenic Republic, Republic of Honduras, Hungary, Islamic Republic of Iran, Republic of Lebanon, Republic of Malta, Republic of the Marshall Islands, Kingdom of Morocco, Republic of the Union of Myanmar, Federal Republic of Nigeria, Republic of Palau, Independent State of Papua New Guinea, Republic of Peru, Republic of Poland, Republic of Slovenia, Republic of the Sudan, Republic of Trinidad and Tobago

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

Acknowledging scam monitors and telecommunication services,

Noting with regret the amount of scam advertisements,

Deeply concerned by the impact cyber-crime has on technologies and devoting attention to studying the limits of technology to advance the safety and security of users online,

Aware that a lack of verification logos could cause users to trust unreliable sites,

Recalling the former intentions of the Ad Hoc Committee in relation to ICT crimes,

Fully aware of the need of global cybersecurity laws to combat cybercrime,

Regretting the fact that many underdeveloped countries lack adequate cybersecurity,

Authentication of information and fostering cognizance

1. Urges the implementation of scam monitors for telecommunication services;
2. Recommends the education of people in the prevention of cyber-crime;

3. Encourages countries to implement firewalls to protect citizens;
4. Strongly encourages the blocking of scam advertisements on websites;
5. Suggests the further protection of ICT users online;

Technological resources

6. Affirms the usage of government issued verification indicators on websites;
7. Advises the use of AI as a cyber resource;
8. Further reminds member states that AI can be useful in the case of ICTs;
9. Recommends stricter regulations on what AI is available to the public;
10. Approves the criminalization of cyber-crime;
11. Calls upon countries to utilize cyber resources;
12. Considers that AI might not always be a trusted source.

Cybersecurity laws

13. Encourages countries to store data in secure locations in order to prevent data leaks;
14. Calls for attempts to track down/identify and remove all scam call centers;
15. Further requests for digital moderators to implement verification systems for website;
16. Suggests an international law that establishes that all tech companies include a free protection program in their devices;
17. Expresses its hope for the creation of an online system that directs cybercrime complaints to the appropriate organization;

Improving the cybersecurity of member states

18. Calls upon countries with strong cybersecurity to promote global equity by lending aid to those lacking adequate cybersecurity;
19. Requests further internet safety by the use of firewalls and virus protection;
20. Urges countries to train judiciaries and law enforcement to combat cybercrime;
21. Endorses the development and preservation of digital infrastructure spanning both national and international scales; and
22. Invites positive digital citizenship with the goal of a safe global community.