Resolution United Nations Office on Drugs and Crime/1.1

United Nations Office on Drugs and Crime Committee

Co-sponsors: Plurinational State of Bolivia, Federative Republic of Brazil, Republic of Colombia, Union of the Comoros, Democratic Republic of the Congo, Republic of Cyprus, Czech Republic, Republic of El Salvador, Gabonese Republic, Federal Republic of Germany, Republic of Ghana, Hellenic Republic, Republic of Guatemala, Republic of Guinea-Bissau, Republic of Indonesia, Republic of Lebanon, Republic of Madagascar, Islamic Republic of Mauritania. Republic of Moldova, Kingdom of Morocco, Republic of Mozambique, Republic of the Union of Myanmar, New Zealand, Republic of Nicaragua, State of Palestine, Republic of the Ukraine, United States of America

Topic: Addressing Cyber Crime to Protect Election Legitimacy

Noting with deep concern how easily misinformation is spread,

Fully aware of the problem of cybercrime because given most countries lack of cybersecurity, this fear is much more evident,

Alarmed by the increasing amount of cyber attacks in the past few years, such as the wancry ransomware of 2018,

Guided by the Budapest convention on cybercrime countries must work together to create treaties to protect nations from cybercrime,

Keeping in mind that Estonia, Guinea-Bissau and some other countries have found success using online voting and government supported poll-watching groups,

Noting with regret the lack of action on the topic of cybersecurity,

1. Calls upon governments to tighten restrictions on media companies in order to prevent the spread of falsified information;

2. Calls upon nations to enforce a more focused effort from their justice systems targeting cybercrime;

3. Emphasizes the need for people of all ages to be educated on the topic of cybercrime by creating cybersecurity programs funded by the UN;

4. Encourages nations to further protect websites and online user information;

5. Recognizing the need for increased legislation to prevent cybercrime;

6. Seeking the creation of a global database that would provide reliable resources to cite sources;

7. Calls upon nations to create protocols that track perpetrators of cybercrime when systems are breached;

8. Endorses the further implementation of more cybersecurity protocols on the internet along with monitoring websites;

9. Recommends that nations ensure the safety of their internet commerce services and most commonly used websites by performing regular security checks on their cloud and web servers in hopes of restricting access to the dark web;

10. Recommends the widespread use of cybersecurity tools such as VPNs;

11. Calls upon member states to create trust between nations by lending assistance and sharing infrastructure, resources and knowledge to enhance international cooperation;

12. Proclaims that the enhancement of communication systems between governments, organizations and national surveillance on online voting is improved so voting officials and voting stations can be alerted if there is a security breach or risk;

13. Recommends countries come together in a summit to brainstorm ways they can fund and protect each other from cybercrime;

14. Encourages member states to create international training centers to train people on how to protect governments from cybercrime during elections by forming cybersecurity agencies and prosecution teams;

15. Supports the act of providing citizens with information to contact the proper agency of cybercrime via a secure website;

16. Encourages all countries to sign and ratify the Counsel of the Europe's Convention on Cybercrime;

17. Requests member states to draw attention to current voting issues in their country and to educate themselves about cyberattacks on the government;

18. Endorses the governmental and UN funding of research into cybercrime to build expertise and increase cyber-protection.