Resolution United Nations Office on Drugs and Crime/1.1

United Nations Office on Drugs and Crime Committee

Co-sponsors: Islamic Republic of Afghanistan, Republic of Armenia, Kingdom of Bhutan, Republic of Cameroon, Canada, Republic of Colombia, Union of the Comoros, Republic of Ecuador, Arab Republic of Egypt, Federal Democractic Republic of Ethiopia, Federal Republic of Germany, Republic of Iraq, Malaysia, Republic of Serbia, Republic of Korea, Democratic Socialist Republic of Sri Lanka

Topic: Addressing Cybercrime to Protect Election Legitimacy

The Committee,

Bearing in mind the widespread availability and accessibility of technology,

Noting with regret since online voting can have a big impact in the future, unfactual political opinions have the ability to change the response of voters, thus creating an unfair democracy,

Keeping in mind that only half of the world has access to the internet and the technology to create an online voting system that will be impermeable to hacking,

Aware of the amount of time, resources, and effort solving this issue will require,

Alarmed by the lack of knowledge and education on cyber crime and the amount of misinformation and insecurity on websites,

Noting with deep concern the minimal actions taken upon the government influence and this worldwide issue about how cyber crime affects election legitimacy,

1. Supports the designation of a group of employees within social platforms through the formation of an international company that serves the purpose of filtering posts and messages on social media platforms in order to differentiate between the permittance of appropriate content and the removal of fake, violent, and unfactual content in elections;

2. Further requests the creation of a software that is implemented either through robot-based (automatic) or committee-based (manual) scans of harmful links or files as a part of social media platforms to detect whether hackers are trying to commit cybercrime in order to prevent hacking from happening;

3. Emphasizes the use of types of identification, specifically an email, phone number, and specific codes from government issued devices to verify whether you are a hacker or regular voter in terms of online voting and to check whether that person has not voted yet in order for the vote to be counted;

4. Requests the implementation of resources such as private passwords that are sent through secured methods such as private emails and phone numbers that are individualized per voter in order to prevent hackers from re-entering and tampering votes;

5. Draws the attention that there is an ability to black-list and white-list within social media for those that post inappropriate or unfactual content, there will be a committee set aside to blacklist them to separate facts from opinions;

6. Further requests member states should have another way to host elections if the online voting platform fails or is hacked;

7. Encourages member countries to create informational campaigns relating to their own elections;

8. Calls upon member states to create an online voting platform that provides resources to help voters navigate the online voting system;

9. Further recommends that member states distribute voting devices to all voters that do not have access to personal devices in order to vote;

10. Supports the African Union's treaty and the European Union's treaty on cyber crime;

11. Requests resolutions or conventions about influence in elections;

12. Calls the United States or the European Union to assist on implementing a strong website to finalize a safe online voting system;

13. Recommends using social media to spread information about election legitimacy;

14. Authorizes schools to educate students about cyber crime and insecure websites through educational programs;

15. Supports access to information regarding safeguards and firewalls;

16. Further encourages the public to report cyber attacks though help lines or websites.