

Committee: Ad Hoc Political and Security

Sponsoring Country: Denmark

Topic: Cybersecurity Standards, and the Digital Defense of Member States

The General Assembly,

Bearing in mind the increase in communications over digital means,

Recognizing that a global culture of digital security that needs to be implemented,

Reaffirming the continuing need to enhance cooperation regarding digital vulnerabilities,

Stressing the need to have an international standard of digital security,

Recalling Resolution 56/121 of January 2002 on Combating the criminal misuse of information technologies, Resolution 57/239 of January 2003 on Creation of a global culture of cybersecurity, Resolution 58/199 of January 2004 on Creation of a global culture of cybersecurity and the protection of critical information infrastructures and, Resolution 64/211 of March 2010 on Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures,

Noting with deep concern the claims of tampering in the government elections of Member States,

Guided by the importance of protecting necessary infrastructure,

Affirming that the use of digitally secure infrastructure is a critical duty of governments,

Taking note the recent data breaches,

1. Emphasizes the requirement for a international standard of cybersecurity practices;

2. Requests the creation of the Hardware And Cybersecurity Knowledge Enterprises for Restoring Safety (HACKERS) subcommittee to oversee the implementation of global cybersecurity standards, and coordinate the digital defense of member states
 - a. This committee will be responsible for
 - i. The publication of a monthly briefing regarding new digital threats
 - ii. Ensuring that all member states meet or exceed agreed upon cybersecurity standards
 - iii. Ensure communication among member states regarding vulnerabilities deemed to be dangerous to national security
 - b. The committee shall be consisted of 5 permanent members and a rotating set of 8 other member states
 - i. The 5 permanent members, based on a 2018 cybersecurity index, are as such
 1. USA
 2. France
 3. India
 4. Denmark
 5. South Korea
 - ii. The rotating members shall be decided upon by the 5 permanent members upon the inaugural meeting of the committee
 - iii. After such a meeting the members shall be chosen by the committee as a whole.
 1. A rotating member's term consists of a 2 year period on the committee after which they are not eligible to serve in the committee for a period of 4 years
 - iv. The dismissal, introduction and, elevation of members

1. The committee must agree with at least $\frac{3}{4}$ ths voting in favor of dismissal
2. The committee must meet as quick as possible, to vote in a new member
 - a. The committee must agree with at least $\frac{2}{3}$ voting in favor of the introduction
 - b. In order to elevate a member to a permanent member
 - i. There must be a position open for the elevation
 - ii. There may only be 5 permanent members at any time
 - iii. The committee must have $\frac{3}{4}$ votes in favor of the member being elevated to a position of permanent member
 - iv. The member must have been a rotating member at least once before in order to be considered for vote
 - c. The committee will also be responsible for advising any council or committee in regards of matters dealing with, or in relation to the topic of cybersecurity, or the apprehension of cyber-criminals
 - d. The committee with also serve to regulate acts of cyber warfare
 - i. Cyber-Warfare is herein defined as
 1. A disruptive act committed by a nation upon another nation with the intention of causing any matter of destruction of or in relation to any digital infrastructure of said attacked nation
 2. Any sort of interference with a nations digital systems resulting in any form of down time
 - e. This committee will also serve to help combat Cyber-terrorism

- i. Cyber-Terrorism is herein defined as any method of cyber-warfare as committed by any individual with or without a political motivation;
3. Authorizes a publication of global security standards to be made publicly available
 - a. The standards shall be defined by the aforementioned committee;
4. Condemns the interference of digital infrastructure of nations states by other nation states;
5. Further reminds member states to cooperative interact with one another in regards to digital vulnerabilities on other nation's digital infrastructure.