**FORUM:** United Nations Security Council (UNSC)
**QUESTION OF:** Investigating developments and risks of Cyber Warfare

THE UNITED NATIONS SECURITY COUNCIL,

*Defines* a cyber attack as any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage,
*Recognises* that cyber attacks can aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems,
*Categorizes* cyber attacks as attacks with criminal, political or personal motives
*Condemns* the actions of individuals involved in the voluntary coding and sharing of malware, finance of any form of cyber attacks and individuals that were aware of any cyber attack prior to its execution,
*Emphasising* the importance of strengthening transnational cybersecurity initiatives so as to better safeguard critical global infrastructure networks from damage as a result of sophisticated cyberattacks conducted by criminal or terrorist groups.
*Recognising* the need for a coordinated international response to tackle the threats posed by organised crime activity in the cyberspace and to reduce the operational capabilities of international criminal syndicates,
*Reaffirming* the commitments of UN member states to ensuring a safe and secure online space as outlined in General Assembly Resolutions 55/63, 56/121, 57/239, 58/199, and 64/211, as well as in Security Council Resolutions 2341 and 2370,
*Recognizing* the increasing threat posed by cyber attacks on critical infrastructure and the potential for such attacks to undermine the economic and social well-being of states
*Acknowledging* the need for greater international infrastructure-building cooperation and information-sharing to prevent and respond to cyber attacks,
*Deeply regretting* the rise of cyberwarfare and cyberattacks all around the world,
*Recognising* the need for substantial support for less developed countries to bolster their cybersecurity defenses,
*Bearing knowledge that* the United Nations General Assembly adopted a resolution to set in motion a process to draft a global comprehensive cybercrime treaty in 2019,
*Guided by* the purposes and principles enshrined in the Charter of the United Nations,
*Determined to* counter the use of information and communication technologies for criminal purposes,
*Considering* the General Assembly Resolution 75/282, which worked on Countering the use of information and communications technologies for criminal purposes;

1. Underlines the necessity of access to cybersecurity for emerging economies and LDCs, through,

a. a request for the creation of the DWCM (Developing World Cyber Security Mechanism) by the UN to fund, educate and facilitate necessary infrastructure development in less economically fortunate states, understanding the need to provide the tools and education necessary in mitigating cybercrime, which disproportionately originates from such,
b. specifying that investments should be addressed in backup systems, redundancies, and disaster recovery plans, as well as efforts to identify and address vulnerabilities in the systems that support our economies and societies;

2. Expresses the need to create national education programs on recognising "disinformation", supported by,
    a. creating an international commission of experts and political leaders to determine the definition of "disinformation", in which the permanent 5 will retain their veto power,
    b. endorsing the support of countries with limited resources in setting up national education programs on recognising "disinformation" through economic support and knowledge-sharing programs;

3. Recommends expanding the department of cybersecurity of the UN office of counter-terrorism, with voluntary participation from national cyber-defence agencies and private cybersecurity companies, to assist with the implementation of a robust cyber-defence mechanism for national governments seeking assistance, in ways such as but not limited to:
    a. formulating a concise and easily comprehensible document outlining the necessary essentials for setting up an effective cyber-defence strategy and outline future guidelines for cybersecurity to facilitate transition of the private sector,
    b. offering tailored guidance to governments, especially from developing countries, who request advice on ways of setting up, expanding or upgrading their cybersecurity infrastructure,
    c. researching stronger cyber protection mechanisms by exploring a broad scope of cybersecurity aspects including but not limited to:
        i. encryption hardware
        ii. anti-breach software
        iii. cyber-defence doctrine
    d. conducting investigations and inquests into past known data breaches to identify weak points and vulnerabilities in firewall code which hackers had been able to exploit;

4. Recognises that the main potential risks related to cyberwarfare are the following,

a. Reputational damages caused to private corporations such as banks, social media, et cetera and/or national states can lead to unfavorable consequences such as economic instability, unease amongst the general population, et cetera,
b. Confidential information breaches leading to potential deterioration of diplomatic relations and increased vulnerability of affected states,
c. Financial losses due to theft and/or deletion of loans,
d. Extreme loss of life following cybersecurity breaches to public health institutions and networks;

5. Decides to remain actively seized on the matter.