FORUM: UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT

QUESTION OF: Measures to Combat International Cybersecurity Attacks

MAIN SUBMITTER: Singapore

CO-SUBMITTERS: India, Cuba, Peru, Djibouti, Dominican Republic, Australia, The Slovak Republic, South Africa, Argentina, UAE

*Aware* of the increasing frequency and severity of international cybersecurity attacks, which pose a significant threat to global security, stability and the integrity of digital networks and infrastructure,

*Recognizing* the universal right to a secure and accessible cyberspace and the need for cooperative efforts to effectively address cyber threats,

*Acknowledging* the challenges and risks posed by information and communication technologies to the protection of rights, such as interception, the potential impact of these attacks on critical sectors such as finance, health care and national security, which can disrupt economies and undermine the sovereignty of States, as well as the threat of cyber-attacks, cyber-warfare and cyber-terrorism,

*Emphasizing* the importance of addressing at the international level issues related to the protection, processing and encryption of information conducted by governments and combating cyber-attacks, cyber-warfare and cyber-terrorism, while upholding human rights and fundamental freedoms,

*Recognizing* the importance of implementing comprehensive measures and international cooperation to strengthen cybersecurity and to prevent, deter and respond to malicious cyber activities,

*Aware* of the annual economic losses caused by cyber-attacks worldwide are approximately $8 trillion, nearly 1 billion emails involving APT (Advanced Persistent Threat) were exposed in a single year, affecting one in five Internet users,

*Noting* that the Budapest Convention assists countries in addressing cyber threats through a coherent global approach,

*Recalling* that the International Organization for Standardization (ISO) has published several cybersecurity standards,

*Requesting* member states to take the following actions in order to take international cybersecurity issues more rigorously and seriously,

*Bearing in mind* that The Budapest Convention aids countries in addressing cyber threats through a cohesive global approach,

*Recognizing* the International Organization for Standardization (ISO) has released several cybersecurity standards,

*Calls upon* member states to take the following actions to in order to take international cybersecurity issues more rigorously and seriously,

1. Urges organization such as The National Cyber Security Alliance (NCSA), The Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) to remind citizens about the seriousness of the cyber-attacks and educate citizens about preventing cyber-attack in such ways but not limited to:
	1. creating non-digital posters to alert citizens about ways to prevent cyber-attacks in ways such as debut not limited to:
		1. the appropriate ways to find secure internet connections,
		2. ways to strengthen passwords;
	2. alerting dangers of cyber-attacks through social medias in such as not limited to:
		1. YouTube,
		2. Social Network Service (SNS) such as Instagram, Twitter, Facebook,
		3. on the news such as CNN and BBC;
2. Strongly request members states to enact new legislation and strengthen existing legislations that promote the punishments to the protection of citizen from the cyber-attacks in such ways but not limited to:
	1. strengthening punishments for cyber-attacks, according to relevant national laws, through measures including, but not limited to:
		1. increase the fine depending on the local laws,
		2. increase the length of prison labor;
	2. requesting all member states governments to ban dark websites and malicious hacking websites;
3. Calls upon national governments of the nations and the International Organization for Standardization (ISO) to engage with numerous industry experts in efforts to promote and enforce internationally recognized, secure coding practices in ways such as but not limited to:
	1. formulating comprehensive secure coding standards that can be globally implemented in ways such as but not limited to:
		1. teaching secure coding practices in colleges and universities,
		2. requiring all IT workers and coders to take a comprehensive test before being accepted into IT and technology companies and corporations;
	2. requesting all software companies to undergo annual safety checks by ethical hackers in ways such as but not limited to:
		1. authorizing and granting certified ethical hackers’ permission to attempt to penetrate a company’s security system to test the quality of the security systems,
		2. allowing ethical hackers to work with members of that company to strengthen the cybersecurity systems of the company;
	3. establishing organizations to spread secure coding awareness to the programming community on code-sharing websites such as but not limited to:
		1. Reddit,
		2. Stack overflow,
		3. GitHub,
		4. DEV community;
4. Urges member states to draft, implement, and regularly update comprehensive national cybersecurity strategies, promoting collaboration with international cybersecurity agencies and experts to fortify defenses against cyber threats in ways such as but not limited to:
	1. calling for the creation of national cybersecurity task forces comprising experts in the field to conduct regular assessments, identify vulnerabilities, and propose solutions to safeguard critical infrastructure and sensitive information:
		1. encouraging the sharing of best practices and technological expertise among member states to ensure the most effective and up-to-date cybersecurity measures are implemented across borders,
		2. suggesting the establishment of educational programs and training initiatives to raise awareness about cybersecurity threats and best practices among government officials, private sector entities, and the general public;
	2. Urging member states to establish a coordinated incident response plan aimed at, efficiently addressing and mitigating the impact of cyber-attacks on a global scale, such as technology and a state secret:
		1. underlining the significance of rapid and unified actions to address cyber threats effectively and minimize their consequences through the implementation of a structured and coordinated incident response plan,
		2. stressing the importance of collaborative efforts and sharing resource such as attack pattern and vulnerabilities among member states to ensure a swift and efficient response to cyber incidents on an international level;
5. Emphasizes the need for the establishment of an international cyber defense consortium, comprising cybersecurity experts from member states, to collaboratively devise, implement, and update a unified framework aimed at countering evolving cyber threats and fortifying global digital infrastructure resilience in ways such as but not limited to:
	1. calling for the consortium to develop a shared database integrating real-time threat intelligence, enabling swift information exchange and coordinated responses among member states:
		1. encouraging the consortium to organize regular cyber defense 3workshops and knowledge-sharing sessions, fostering expertise exchange and skills. development among member states' cybersecurity professionals,
		2. suggesting the creation of a standardized incident response protocol to be adopted uniformly a cross member states, ensuring a cohesive and efficient approach to mitigate cyber-attacks on a global scale;
	2. calling for the committee to develop a comprehensive capacity-building program focused on enhancing cybersecurity awareness, skill development, and resource allocation, particularly in developing nations, to ensure a more inclusive and globally fortified cyber defense network, emphasizing the necessity for targeted educational initiatives and mentorship programs within the capacity-building program to empower developing nations in addressing cyber threats, thus bridging the digital security gap between countries;
6. Create compulsory free education to teach how to prevent cyber-attacks which citizen can take the session and provide practice so that citizens completely understand how to react but not limited to:
	1. encouraging NGOs to take a video that shows the ways to prevent cyber-attacks,
		1. showing different types of cyber-attacks and different ways to prevent cyber-attacks for each type,
		2. showing what to do if citizens accounts are compromised by cyberattacks;
	2. requesting organizations to use social medias to show the ways to prevent cyber-attacks.