Delegate Name: Alex Kalathil Arun

Country: Syria

Institution: UNSC

Topic: Assessing and Mitigating the Dangers of Cyberattacks

“Cyber security is not a one-time task; it is continuous process assessment, adaptation and mitigation.”

Assessing and mitigating the dangers of cyber-attack is important in todays interconnected world. As the use of technology increases, the risk associated with cyber threats also increases. These dangers broaden a wide range of malicious activities like data breaches, ransomware attacks, and the disruption of critical infrastructure. To bring down these issues the UN has taken some important steps to address cybersecurity on a global scale. The UN promotes global collaboration and dialogue to improve cybersecurity measures through initiatives like the UN Group of Governmental Experts on Information and Telecommunications Security. Moreover, the UN promotes capacity-building efforts to help member states in assessing their vulnerabilities and developing great strategies for mitigating cyber threats. By bringing collaboration among nations and facilitating the exchange of best practices, the UN plays a vital role in safeguarding the digital world against the dangers posed by cyberattacks.

Syria ranks 31 out 100 countries in the world for having the lowest level of safety against cybercrime. The Syrian conflict has had a significant impact on the country's cybersecurity. Over the past few years, Syrian hackers have become increasingly active, launching cyber-attacks on businesses and organizations globally. They have targeted everything from news agencies to government websites. There are some actions taken by the Syrian Government regarding the cyber-attacks and cyber security. In recent years, it has intensified efforts to control online communication and combat perceived cybercrimes. The government launched measures that have chilling effects on online discourse, thus journalists and activists from foreign countries have faced risk due government monitoring.

As the delegate of Syria, to avoid cybercrimes we must bring awareness about cyber safety to the people who have less knowledge about cybercrimes. We can do this by setting up posters or by posting videos about cyber awareness throughout the country and how to fight against cyber-attacks. The government should also try to improve the safety features of online public services like online banking, online shopping and many more. The government should also take serious actions against the once who do malicious things to get private government properties. For these and many more, the above are some the important solutions that can help make Syria a safer cyber country.

Thank you

Bibliography:

<https://timep.org/2022/10/05/understanding-assads-new-cyber-crackdown-in-syria/>

<https://snhr.org/blog/2021/10/14/56921/>

<https://seon.io/resources/global-cybercrime-report/>

<https://syriadirect.org/cyber-attacks-and-surveillance-in-assads-syria-they-can-do-whatever-they-want-they-own-the-infrastructure/>

<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf>

<https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211037/full/html>