Position Paper



**Name**: Neiyl Sagar Vasishta

**Allocation**: Russian Federation

**Institution:** Welham Boys’ School

**Agenda**: Assessing and Mitigating the Dangers of Cyber Attack

Introduction:

The Russian Federation considers Cyber Attacks a grave threat to our international security and thriving economy. To address the challenge, Russia advocates for enhanced and strengthened international cooperation. This includes increased information being shared among countries to track down the catalysts of cyber-attacks. The Russian Federation emphasises the importance of establishing international guidelines for the responsible behaviour of nations present in cyberspace. However, we are viewed with scepticism by a significant portion of the international community. This creates an environment of uncertainty and distrust, hindering international cooperation and stability.

The Threats of Cyber Attacks:

Cyber-attacks can transcend national borders, targeting critical infrastructure, finance institutions and sensitive data. These attacks can disrupt a person’s life, cause economic hardship and might as well destroy a country. The anonymity afforded by cyberspace allows malicious actors both national and international to operate with exemption. For example, in 2021 during the Covid Era, a major credit card company suffered a cyber-attack where hackers accessed the personal information of millions of customers. Moving to social media platforms, these platforms are vulnerable to cyber-attacks that spread fake news or propaganda. This can manipulate public opinion and undermine trust in democratic processes. As the delegate of the Russian Federation, I’d like to say that these attacks can be a serious problem, and everyone needs to work together to stop them.

Solutions Proposed by Russia:

* **Information Sharing:** Improved communication and intelligence sharing among member states are crucial for identifying and tracking down the catalysts of cyber-attacks. This collaborative effort will encourage a more coordinated response and facilitate attribution for antagonistic activities.
* **Establishing International Morals:** The international community needs to establish clear ethics for responsible state behaviour in cyberspace. These morals should discourage aggressive actions and promote trust and predictability between nations.
* **Multilateral Dialogue:** Regular dialogue and diplomacy are essential for building trust and fostering cooperation on cyber security issues. Russia believes in establishing dedicated forums within international organizations to discuss cyber threats, share information and defend one's information.

Conclusion:

The Russian Federation remains committed to working with the international community to create a safer and more secure digital environment. The fight against cyber-attacks demands a United global front. By adopting a collaborative approach focused on information sharing, establishing international morals and maintaining open dialogue the international community can effectively oppose the dangers posed by cyber-attacks and ensure a stable and secure world.

**BIBLIOGRAPHY**

* <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia>
* <https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf>
* <https://www.imperva.com/learn/application-security/cyber-security-threats/>
* <https://www.cia.gov/the-world-factbook/>

Thank You,

The Russian Federation