POSITION PAPER

Committee: The United Nations General Assembly (UNGA)
Topic: Advancing responsible state behavior in cyberspace in the context of International Security
Country: Japan
Delegate: Parth Gurjar (Delhi World Public School, Noida Extension)

The term cyberspace has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. It is a concept describing a widespread interconnected digital technology.

While there is no internationally accepted definition of cybersecurity, the dominant discourse around the world, promoted by policy-makers and government agencies, focuses on international crime, prevention of terrorism and the quest for ever increased surveillance of our communications and data.

Cyber security is important for entire world because it protects all categories of data from theft and damage. This includes **sensitive data, personally identifiable information, protected health information, personal information, intellectual property data, and governmental and industrial information systems.**

The control of cyberspace is thus important not only because of the actions of individual participants but because the infrastructure of cyberspace is now fundamental to the functioning of national and international security systems, trade networks, emergency services, basic communications etc.

Information technology is transforming modern life, driving innovation and productivity, facilitating the sharing of ideas, of cultures, and promoting free expression. Its benefits have brought the global community closer together than ever before in history.

Country Policy:

The purpose of the Basic Cyber security Act to move cyber security related policies forward in a comprehensive and effective manner, and contribute to the creation of a more energetic and continuously developing economic society, consequently contributing to the national security of Japan.

As a responsible states Japan upholds the international rules-based order, we recognize our role in safeguarding the benefits of a free, open and secure cyberspace for future generations.

When necessary, Japanese government will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace.

Based on the Japan Revitalization Strategy and the Cyber Security Strategy developed in June 2013 and summarizes Japan's basic policy and its priority areas for international cooperation and mutual assistance in the field of cyber security, outlining four basic principles:

- Ensuring the free flow of information
- Responding to increasingly serious risks
- Enhancing risk-based approach
- Acting in partnership based on social responsibilities

Outlined Priority Areas for international cooperation are -:

- Implementation of dynamic responses to cyber incidents
- Building up "fundamentals" for dynamic responses
- International rulemaking for cyber security

Possible Solutions:

We categorize solutions to the global cyber security problem based on the main enablers of cyber issues. The two main categories are technology and regulation-enabled solutions. The implementation approach further refines this taxonomy.

Technology-enabled solutions
A typical Web transaction involves a Web client and a Web server. We classify technology-enabled solutions according to the type of Web entities that are responsible for their implementation: clients, servers, or clients/servers.

Regulation-enabled solutions
Regulation-enabled solutions encompass two types: self and mandatory regulation solutions. Self-regulation refers to the information keepers' ability to voluntarily guarantee data security. Mandatory regulation refers to legislation aimed at protecting citizen's security while they transact on the Web.

In addition of that, A shared global database of cyber processes that can improve transparency on what each process does, who participates, and how its work is received in other processes that is, what sort of cross-pollination is occurring versus triggering competing or conflicting norm proposals. In this regards, the UN can play a significant role in preparation, implementation and monitoring of appropriate and comprehensive norms for every responsible state.

Conclusion:

The internet was not designed with security at top of mind. It was built to spread information, not contain it, and has in succeeded at this central objective in spectacular fashion. As the internet and digital economy mature, however, cyber security is now rising on the list of priorities for consumers and increasingly for policy makers as well.

We hope that the situation might improve for the cyber world, but the future appears bleaker. Since the advent of a digital society with online accounts, organizations that harvest user data have amassed tremendous powers. While certain merits can be argued for collecting user data, an equivalent responsibility remains to regulate and secure any stored digital data.

The UN must be proactive and provide a sturdy forum for all states globally. It is the responsibility of the international community to foster cyber security-enhancing technologies that will protect all countries equally.