Forum: Security Council (SC)

Issue: Promoting the Development of Cyber Resilience Within Government Agencies

Chairs: Hala Al Sailani & Amal AlNaggar

Introduction

As the creation and development of advanced technology progresses, governments have proportionally adjusted to the changing times and implemented these technologies into their multi-faceted societies.This rise in technology, however, has simultaneously promoted a new platform through which cyber terrorists can breach nations' peace and security. The United Nations has spoken on behalf of these recent exponential increase in cyberattacks, citing countries' healthcare sectors experiencing ransomware and even cybersecurity attacks in their own specialized agencies' IT infrastructures, thus arousing fear among government agencies. While the creation of advanced impregnable network security devices can extinguish this fear and reduce cyber attacks, fortifying cybersecurity and developing cyber resilience in existing technology quenches the issue more effectively. Working towards developing systems resistant to the consequences of security breaches will result in more resilient government agencies and a safer world. This document aims to present the United Nations' relation with encouraging cyber resilience and to promote possible routes through which perseverance in the midst of terrorism can be established.

Definition of Key Terms

Cyber Resilience

Technology's ability to perform correctly and deliver required output despite breaches of cybersecurity (e.g. cyber attacks).

Cyber Security

The means through which technology, its frameworks and inner workings are shielded from digital attacks.

General Overview

With the continuous evolution and modernization of technology in both the United Nation systems and nations' own government agencies comes an increase in proportionately modern means of terrorist attacks through technological means. These cyberattacks pose a threat to various sectors of Member States' societies, ranging from basic IT systems to agriculture. The UN has thus gone through lengths to not only improve cyber security and resilience amongst its own systems, but also to promote such developments in Member States' departments. The fundamental steps to such progress commenced in 2010 which consisted of major action taken by the Chief Executive Board for Coordination (CEB) and its two high-level committees. These actions resulted in mutual consensus made by these specialized committees and other UN agencies on the profound concerns cyberattacks raise and the need for awareness and defense against them. Following into the next decade, the UN's agencies endorsed various frameworks and mandates to be acknowledged and adopted by delegations. These efforts were officially unified in the drafting of a convention by a UN assembly that outlines the principles and methods to uphold cyber resilience and safety.

Major Parties Involved

The United States of America

- The United States shared remarks during a Security Council Arria-formula meeting it co-hosted, commenting on the delegations' vision of sustaining a

technologically-advanced society with the promotion of cybersecurity and resilience. The delegation additionally shared its concerns of other countries' relations with cybercrime, and further highlighted the United States' readiness in cooperating to achieve complete safety;

- The country also established its own specialized agency known as the Cybersecurity & Infrastructure Security Agency (CISA) whose aim is to support digital safety through identifying states' needs in improving their technological structures. This goal of maintaining cybersecurity is acknowledged every November with the month promoting Critical Infrastructure Security and Resilience, focused on emphasizing the crucial role technological infrastructure plays in overall security and resilience to all government levels;
- The United States' is considered a prominent participant in the global effort to instill cyber resilience through its efforts in establishing related agencies, encouraging security in relevant forums, and remaining alert in cyber crime activities by other Member States

Canada

- The National Cyber Security Strategy (NCSS) was established by Canada in 2018 with three fundamental cyber goals: to possess productive collaboration and discipline, to cultivate a compatible flexible cyber ecosystem, and to have resilient and secure systems within the country;
- Canada's department leaders have urged the NCSS to formulate strategies aligned with their primary goals to further the cybersecurity and resilience support on Canadian systems, and have created action plans detailing the roadmap the organization will take to accomplish these goals;

- Canada's engagement in national agendas focused on cultivating and maintaining cyber resilient systems and the government's active participation in such plans showcases the delegation's passion in securing its cyber frameworks to reach national cybersecurity and safety.

Timeline of Key Events

Date	Description of Event
September–October 2010	The threats to cybersecurity in regards to the UN's organizations as well as Member States are discussed during the CEB's twentieth session. These discussions set in motion the consequent operations on reinforcing cybersecurity and the following frameworks recommending cyber resilience strategies.
November 2014	The UN's Cybercrime and Cybersecurity framework is drafted by the High-level Committee for Management (HLCM) and High-level Committee for Programme (HLCP).
August 2024	Through the assistance of the United Nations Office on Drugs and Crimes (UNODC), the Third General Assembly drafts a convention on cybercrime, consisting of tools Member States can adopt to strengthen cyber security and resilience via international, governmental, and technical efforts to defend against cybercrime.

Previous Action Taken

1. The Open-Ended Group (OEWG) was incepted in December of 2010 by the General Assembly. The group invites the collaboration of all Member States and intends to elaborate on and amend pre existing instruments. In the context of cybersecurity, the OEWG suggests principles, normatives, and rules on the action Member States can execute to reinforce their delegations' cybersecurity;
2. In 2021, "Cybersecurity in the United Nations System Organizations" was published by the Joint Inspection Unit (JIU) after its planning, approval, and endorsement by the CEB, HLCP, and HLCM. The report highlights the common challenges the UN system agencies and States encounter with the reinforcement of their cybersecurity and identifies agencies that accommodate wide-spread cybersecurity solutions to potentially share with collaborating departments.

Possible Solutions

1. **National Agency Collaboration**

   Holding conferences or summits hosted by two countries' cyber resilience agencies to promote cybersecurity and resilience-related agency implementation in other countries;
2. **Frequent Targeted Discussions**

   Conducting periodic sessions among assemblies wherein Member States' progress on national cyber resilience implementation is discussed and elaborated on to update the UN and fellow States of effective implementation actions;
3. **Publishing of Cybersecurity and Resilience Guidelines**

Creating fixed documents outlining the best actions in strengthening cybersecurity and resilience in government agencies to further guide and encourage delegations to practice it themselves;

4. **Specialized Aid for In-Need States**

   Focusing on equipping States with less-developed or weaker cybersecurity networks with proper reinforcement tools and installations to fortify individual department security.

Bibliography

Chief Executive Board for Coordination. (n.d.). *Cybersecurity | United Nations - CEB*. Unsceb.org. https://unsceb.org/topics/cybersecurity

Chief Executives Board for Coordination. (2010). *Report of the High-level Committee on Programmes on its twentieth session*. https://unsceb.org/sites/default/files/imported_files/Content/Reports/REP_HLCP_201109_CEB20106_0.pdf

Cybersecurity & Infrastructure Security Agency. (2023a). *Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA*. Www.cisa.gov. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Cybersecurity & Infrastructure Security Agency. (2023b, November 3). *Critical Infrastructure Security and Resilience Month | CISA*. Www.cisa.gov. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-security-and-resilience-month

General Assembly. (2018). *Resolution adopted by the General Assembly on 5 December 2018*. https://digitallibrary.un.org/record/1655670/files/A_RES_73_27-EN.pdf

General Assembly. (2021). *Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report*. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Joint Inspection Unit. (2021). *Cybersecurity in the United Nations system organizations Report of the Joint Inspection Unit Prepared by Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy*. https://documents.un.org/doc/undoc/gen/g21/293/94/pdf/g2129394.pdf

Public Safety Canada. (2023). *Parliamentary Committee Notes: Cyber Security and Protecting Canada's Critical Infrastructure*. Publicsafety.gc.ca. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240614/19-en.aspx

Tolppa, M. (n.d.). *First UN OEWG concludes with a consensus report- what does it mean for the future cyber security discussions under the auspices of the First Committee?* Ccdcoe.org. https://ccdcoe.org/library/publications/first-un-oewg-concludes-with-a-consensus-report-what-does-it-mean-for-future-cybersecurity-discussions-under-the-auspices-of-the-first-committee/

United Nations Office on Drugs and Crime. (2024, August 9). *United Nations: Member States finalize a new cybercrime convention*. United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

United States Mission to the United Nations. (2023, May 25). *Remarks by Ambassador Linda Thomas-Greenfield at a UN Security Council Arria-Formula Meeting Co-Hosted by the United States on Cybersecurity*. United States Mission to the United Nations. https://usun.usmission.gov/remarks-by-ambassador-linda-thomas-greenfield-at-a-un-security-council-arria-formula-meeting-co-hosted-by-the-united-states-on-cybersecurity/