ETMUN

Unraveling the Domino Effect

Committee: Security Council

Topic: Addressing the Global Impact of a Large-Scale Cyberattack on Critical Infrastructure and Its Potential for Triggering Regional and Global Instability.

President: Zaid Khawaj

Deputy President: Taj Bustanji

Chair: Raya Majdalawi

Table of Content:

Letter from the President:

Dear Esteemed Delegates,

I extend my warmest greetings to each of you as the President of the Security Council for this Model United Nations session. It is my distinct honor to preside over what promises to be a dynamic and engaging forum.

Your participation adds a valuable dimension to the council, and I am confident that your unique perspectives will contribute to fruitful debates and resolutions. Let us embrace the spirit of diplomacy, cooperation, and dialogue as we work together towards addressing the pressing issues before us.

I encourage you to actively engage, express your thoughts, and challenge each other's ideas with respect and consideration. Remember, it is through robust debate that we forge lasting solutions.

I look forward to witnessing your intellectual prowess and diplomatic finesse in the coming days. Together, let us make this MUN experience both educational and enjoyable.

Best regards,

Zaid Khawaj

Security Council President

Definition of Key Terms:

Large-Scale Cyberattack:

A coordinated and widespread assault on digital systems, often involving the unauthorized access, disruption, or destruction of information technology infrastructure

Critical Infrastructure:

Essential systems and assets, both physical and virtual, such as energy, water, transportation, and communication, whose incapacitation would have a debilitating impact on national security, public safety, and economic well-being.

Global Impact:

The far-reaching consequences that extend beyond national borders, affecting multiple countries, industries, and aspects of society due to the interconnected nature of the modern world.

Regional Instability:

Disruption or turmoil within a specific geographic area, arising from the compromised functionality of critical infrastructure, potentially leading to social, economic, or political unrest.

Global Instability:

The broader disruption and disorder on an international scale resulting from a large-scale cyberattack on critical infrastructure, impacting diplomatic relations, trade, and global stability.

Cybersecurity Resilience:

The capacity of a system, organization, or nation to anticipate, prepare for, respond to, and recover from a cyberattack, minimizing the impact on critical infrastructure and overall stability.

Deterrence Measures:

Strategies and actions aimed at discouraging potential cyber adversaries by showcasing the ability to identify, attribute, and respond effectively to cyber threats.

Collaborative International Response:

Cooperative efforts among nations, organizations, and cybersecurity entities to address and mitigate the consequences of a large-scale cyberattack, emphasizing information sharing and coordinated countermeasures.

Risk Mitigation:

Proactive measures taken to reduce the likelihood and impact of a cyberattack on critical infrastructure, encompassing preventive cybersecurity measures, incident response planning, and recovery strategies.

Digital Forensics:

The systematic examination of digital evidence following a cyber incident, crucial for understanding the nature of the attack, identifying perpetrators, and improving cybersecurity defenses.

General Overview:

The topic centers on the urgent need to address the global ramifications of a large-scale cyberattack on critical infrastructure, emphasizing its potential to induce regional and global instability. Delegates are expected to delve into the multifaceted challenges posed by such cyber threats, ranging from economic disruptions and compromised national security to potential cascading effects across borders. The committee must explore comprehensive strategies to enhance cybersecurity measures, establish international cooperation frameworks, and develop mechanisms for swift response and recovery. Key considerations should include the identification of vulnerable sectors, the role of state and non-state actors, the legal and ethical dimensions of cyber warfare, and the development of norms to govern cyberspace. Delegates are encouraged to collaboratively draft resolutions that foster a united front against cyber threats while respecting the sovereignty of nations. The committee's ultimate goal is to formulate a robust and adaptive framework that effectively mitigates the impact of large-scale cyberattacks on critical infrastructure, ensuring global stability and resilience in the face of evolving cyber threats.

Major Parties Involved:

Major countries involved in addressing the global impact of a large-scale cyberattack on critical infrastructure include the United States, China, Russia, and members of the European Union. Key people may include government officials, cybersecurity experts, and diplomats, such as those from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), China's Cyberspace Administration, and Russia's Federal Security Service (FSB). International collaboration is crucial to mitigate the potential for regional and global instability arising from such cyber threats;

- The United Nations: Is actively discussing and addressing the global impact of large-scale cyberattacks on critical infrastructure to mitigate potential regional and global instability. Efforts include international cooperation, cybersecurity measures, and diplomatic initiatives to enhance resilience and response capabilities.
- United States of America: Is actively working on bolstering cybersecurity measures to mitigate the global impact of large-scale cyberattacks on critical infrastructure. Efforts include enhancing defenses, international cooperation, and developing response strategies to prevent regional and global instability stemming from such incidents.
- China: It actively working on strengthening its cybersecurity measures to mitigate the risks associated with large-scale cyberattacks on critical infrastructure. The global impact of such attacks is a concern for international stability, prompting countries to collaborate on cybersecurity initiatives. China has expressed commitment to addressing these challenges through diplomatic channels, international cooperation, and the development of robust cybersecurity frameworks. Ongoing efforts involve enhancing cyber defense capabilities and fostering dialogues to establish norms in cyberspace to prevent conflicts and ensure global cybersecurity resilience.
- Russia: Being a major player in the international arena, it has the potential to significantly impact global stability through its actions in cyberspace. A large-scale cyberattack on critical infrastructure could have cascading effects, triggering regional and even global instability. The implications range from economic disruptions to strained diplomatic relations, emphasizing the need for international cooperation to address and mitigate cyber threats effectively.

Timeline of Events:

- **2020**
  - → August: Chinese hackers breached communications networks at a U.S. outpost in Guam. The hackers were able to access sensitive information, including military plans and operations.
  - → December: A group of Russian hackers targeted the SolarWinds software company. The hackers were able to insert malicious code into SolarWinds' Orion software, which was used by a number of U.S. government agencies and businesses. This attack was one of the most sophisticated and damaging cyberattacks in history.
- **2021**
  - → May: Chinese hackers targeted Kenyan government ministries and state institutions, including the presidential office. The hackers were able to access sensitive information, including financial data and government communications.
  - → July: A group of ransomware hackers attacked the Kaseya software company. The hackers were able to encrypt data on the company's servers and demand a ransom payment. This attack affected thousands of businesses around the world.
  - → December: A group of Iranian hackers targeted the U.S. power grid. The hackers were able to gain access to the control systems of several U.S. power plants, but they were not able to cause any outages.
- **2022**
  - → February: Chinese hackers launched a major cyberattack on the International Committee of the Red Cross. The hackers were able to access sensitive information, including medical records and donor lists.
  - → March: A group of Russian hackers targeted Ukrainian government agencies and infrastructure. The hackers were able to cause widespread outages of government websites and critical infrastructure.

- → June: A group of ransomware hackers attacked the JBS meatpacking company. The hackers were able to encrypt data on the company's servers and demand a ransom payment. This attack disrupted the global food supply chain.

❖ **2023**

- → January: Saudi Aramco was hit by a major data breach. The hackers were able to access and steal sensitive information, including oil production data and customer information.
- → March: A massive cyberattack hit Bermuda's Department of Planning and other government services. The attack caused widespread outages and disrupted government operations.
- → October: A group of Indian hackers targeted the US Airport websites and caused disruption in services.
- → October: A group of Russian hackers stole thousands of documents from the British Ministry of Defense and uploaded them to the dark web.
- → November: A group of Indian hackers exploited the CVE-2023-34362 vulnerability in the MOVEit software and stole 815,000,000 records from the Indian Council of Medical Research (ICMR).

Possible Solutions:

1. ***Stresses*** the importance of strengthening Cyber Security Measure among different nations and territories by doing the following:
    a. Improving National Cybersecurity Frameworks by considering the following but is not limited to;
        i. Adding comprehensive legislation to address cyber threats at national levels,
        ii. Updating and strengthening the states legal frameworks to better prosecute cybercriminals involved in attacks on critical infrastructure;
    b. Setting obligation for different nations to abide by the Cyber Security Measures which will have ramifications and sanctions if not followed that include the following:
        i. According to the offence committed, a value decided by board members will be paid;
        ii. Double offenses will meet sanction that are related to trade restrictions and benefits from other nations.
2. ***Encourages*** the promotion of online information sharing, by considering the following measures that include but are not limited to;
    a. Establishing an international mechanism for timely and secure sharing of cyber threat intelligence governed by different persons from around different countries to ensure objectivity and balance;
    b. Building public-private partnerships to foster collaboration in identifying and mitigating potential cyber threats;

3. ***Reaffirms*** the development of international cooperation by the establishment of a Global Cybersecurity Task Force which includes;
    a. Board members from varying regions whose expertise lies in analyzing and responding to large-scale cyberattacks,
    b. Diversifying the board members to incorporate expertise from technical, legal, and diplomatic domains to tackle different forms of crisis,
    c. Developing rapid response protocols for the task force to coordinate international efforts in the aftermath of a cyberattack,
    d. Stressing the importance of swift and collaborative action to minimize the cascading effects of such attacks on global stability,
4. ***Endorses*** the enhancement of critical infrastructure resilience to abide by the following but is not limited to;
    a. International standards to be followed for critical Infrastructure protection by;
        i. The development of international standards for securing critical infrastructure against cyber threats,
        ii. The member states to ensure compliance with these standards and regularly assess and update their critical infrastructure protection measures;
    b. Capacity building and technical assistance by;
        i. Providing technical assistance and capacity-building support to developing nations in enhancing their critical infrastructure resilience.
        ii. Establishing a collaborative platform for sharing best practices and lessons learned in protecting critical infrastructure from cyber threats.

Guiding Questions:

- How vulnerable is our current critical infrastructure to large-scale cyberattacks, and what key sectors are most at risk?
- What potential cascading effects could arise from a significant cyberattack on critical infrastructure, both within a region and globally?
- How effective are current international frameworks and collaborations in responding to and mitigating the consequences of a large-scale cyberattack on critical infrastructure?
- What role do government agencies, private sector entities, and international organizations play in preventing and responding to cyber threats on critical infrastructure?
- How can nations enhance their cybersecurity resilience to minimize the potential for regional and global instability in the aftermath of a cyberattack?
- In what ways might the interconnected nature of global critical infrastructure contribute to the rapid spread of disruptions following a cyber incident?
- What ethical and legal considerations should guide international responses to cyberattacks on critical infrastructure, particularly concerning attribution and retaliation?
- How can advancements in technology, such as artificial intelligence and blockchain, be leveraged to strengthen the cybersecurity posture of critical infrastructure systems globally?
- Are there historical precedents or case studies that offer valuable insights into the potential consequences of large-scale cyberattacks on critical infrastructure and subsequent global stability?
- What measures can be implemented to foster international cooperation and information sharing to proactively address cyber threats against critical infrastructure?