Cybersecurity Committee, PRAMUN 2026 Synopsis

Topic: Countering State-Sponsored Cyberattacks on Critical Infrastructure

## I. Background Information

As societies become increasingly digitalized, cyberspace has evolved into a vital domain that underpins nearly all aspects of modern life. Critical infrastructure—including energy systems, water supplies, transportation networks, healthcare services, financial systems, and communication networks—now relies heavily on interconnected digital technologies. While this connectivity has improved efficiency and global integration, it has also introduced new vulnerabilities.

State-sponsored cyberattacks have emerged as one of the most significant cybersecurity threats facing the international community. Unlike cybercrime conducted for financial gain, these attacks are often politically or strategically motivated and are carried out or supported by national governments. Their objectives may include espionage, disruption, coercion, or the demonstration of technological power.

Cyber operations targeting critical infrastructure are particularly dangerous due to their potential to cause widespread societal harm. Attacks on power grids can leave millions without electricity, cyber intrusions into hospitals can disrupt life-saving care, and interference with water treatment systems can threaten public health. Unlike conventional attacks, cyber operations can be conducted remotely, continuously, and anonymously, often without immediate detection.

Another defining challenge of state-sponsored cyberattacks is attribution. Determining responsibility is technically complex, as attackers frequently disguise their identities through proxy servers, third-party actors, or false digital signatures. This ambiguity complicates diplomatic responses and increases the risk of escalation or retaliation based on incomplete information.

As more states develop advanced cyber capabilities and as global reliance on digital infrastructure grows, the international community must address how to prevent cyber conflict, protect civilian systems, and promote responsible behavior in cyberspace.

## II. United Nations Involvement

The United Nations has played a central role in shaping international dialogue on cybersecurity, even though no binding global cybersecurity treaty currently exists. Through forums such as the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), the UN has worked to establish shared understandings of responsible state behavior in cyberspace.

These UN bodies have affirmed that existing international law, including the principles of sovereignty and non-intervention, applies to state conduct in cyberspace. They have also promoted voluntary norms, including the commitment to refrain from targeting critical civilian infrastructure during peacetime and to cooperate in responding to significant cyber incidents.

Additionally, the UN encourages confidence-building measures such as information sharing, transparency regarding national cyber strategies, and capacity-building initiatives for states with limited cybersecurity resources. Specialized UN agencies and partnerships support technical assistance, cybersecurity education, and resilience-building efforts worldwide.

Despite this progress, major challenges remain. Disagreements persist over governance models for cyberspace, standards for attribution, and the balance between national security and global cooperation. The Cybersecurity Committee, therefore, plays a crucial role in advancing dialogue, proposing norms, and strengthening international cooperation in this rapidly evolving field.

## III. Bloc Positions

Most states agree that cyberattacks on critical infrastructure pose a serious threat, but they differ in how responsibility and prevention should be addressed.

Many Western and technologically advanced states emphasize accountability, transparency, and international norms that restrict malicious cyber activity. They often support collaborative attribution mechanisms, public condemnation of confirmed attacks, and the development of shared cybersecurity standards for critical infrastructure protection.

States such as China and Russia tend to prioritize state sovereignty and caution against mechanisms that could be used to justify external interference or politicized accusations. These countries generally advocate for greater state control over information space and favor the negotiation of comprehensive international agreements governing cyberspace.

Developing states frequently highlight the cybersecurity capacity gap. With limited technical resources, they are more vulnerable to cyberattacks and cannot often detect or respond effectively. These states typically support initiatives focused on capacity-building, technology transfer, and international assistance.

IV. Questions to Consider

When writing your Position Papers and Draft Resolutions, delegates should focus on the following questions:

- What is my country's official position on state-sponsored cyber operations and cybersecurity governance?

- How does my country define and prioritize the protection of critical infrastructure in cyberspace?

- Has my country been a victim of, accused of, or involved in significant cyber incidents affecting critical infrastructure?

- What UN initiatives, resolutions, or working groups related to cybersecurity has my country supported or opposed?

- Does my country favor binding international agreements, voluntary norms, or state-led regulation in cyberspace?

- How does my country approach the issue of attribution and accountability for cyberattacks?

- What role do sovereignty and non-interference play in my country's cybersecurity policy?

- Does my country possess advanced cyber capabilities, or does it rely on international cooperation and capacity-building?

- How do alliances, regional organizations, or geopolitical interests influence my country's stance on cybersecurity?

- Are there statistics, national strategies, or past cyber incidents that support my country's position?

Delegates are encouraged to research information specific to their assigned country and develop a thorough understanding of its cybersecurity policies, capabilities, and strategic priorities. Knowledge of previous cyber incidents, UN discussions, and international norms is essential, as these may directly inform debate and resolution-building. Additionally, understanding the positions of other states will help delegates anticipate challenges and identify opportunities for cooperation.

V. Sources and Useful Links

United Nations Office for Disarmament Affairs – Cybersecurity
https://disarmament.unoda.org/cybersecurity/%5d(https:/www.un.org/disarmament/cybersecurity/)

UN Open-Ended Working Group on ICT Security
https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/75/240]%28https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/75/240%29

Council on Foreign Relations – Cyber Operations Tracker
https://www.cfr.org/cyber-operations/

Center for Strategic and International Studies – Significant Cyber Incidents
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents]%28https:/www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents%29

United Nations Convention against Cybercrime
https://www.unodc.org/unodc/cybercrime/convention/home.html