The General Assembly Blue: Topic A Primary Sources

Protecting sovereign states from international cyber security attacks

Here are primary sources that your moderator or legal chair thought would be helpful in gaining an understanding of the topic. These are by no means all of the sources available, just sources we wanted to highlight.

Source #1: **General Assembly Combating Misuse of Information Technologies (Resolution 55/63)**

This resolution provided an initial push to improve and increase the awareness of the need for cybersecurity throughout the world. It outlines how nations should address the cybersecurity within their own nations and across the world. Delegates should look at this resolution as an opportunity to understand the entirety of international legislation on cybersecurity.

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

Source #2: **Creating Global Culture of Cybersecurity (Resolution 57/239)**

This resolution by the General Assembly recognizes the increasing dependence of the world on internet access. The resolution also recognizes the increasing threat that cyber-attacks present due to the reliance on internet. There is a call for an international effort to defend against cyber-attacks as they require more than just improved technology, but relies on planning and management as well. Delegates should recognize the importance of unifying more than just their government around cybersecurity, but also the organizations and citizens within their country.

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

Source #3: **Protection of Critical Information Infrastructures (58/199)**

This resolution builds off Resolution 57/239, as it encourages international organizations and their respective countries to join in protecting their critical information infrastructure. Furthermore, an annex is provided with "elements for protecting critical information infrastructures". Delegates should recognize these elements and ensure their nation and international organizations are complying.

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

Source #4: **Monitoring the National Efforts to Increase Cyber Security (Resolution 64/211)**

Resolution 64/211 introduces the voluntary self-assessment tool to determine each nation's needs and strategies for cybersecurity. The self-assessment tool looks at the roles and responsibilities of stakeholders, process and participation of policies, the cooperation between public and private entities, management and recovery of incidents, legal frameworks, and the nation's cybersecurity culture. Each delegate should analyze these aspects of their nation to ensure greater security.

https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

Source #5: **UN Group of Governmental Experts Explanation of Developments in Cybersecurity (58/199)**

The United Nations appointed 15 experts from countries that consisted of five members of the Security Council and 10 other member nations. The experts were mandated to study possible cooperative measures in addressing existing and potential threats to cybersecurity throughout the world. This specifically highlights the need to build on confidence-building measures and norms, rules, or principles of appropriate behavior of nations. Delegates should analyze the discussion to understand the future path of international action towards cybersecurity.

https://usun.state.gov/remarks/7880

Source #6: **Addressing Threats against Critical Infrastructure (Resolution 2341)**

This resolution from early 2017 seeks to raise awareness and continue discussion on terrorist attacks against critical infrastructure. It specifically addresses attacks by organizations with highly intelligent personnel through cyberspace. There is also a general understanding that these scenarios vary and are unpredictable, requiring a complete international effort. Delegates should also reference the stances of each nation on cybersecurity within the document when preparing for this topic.

https://www.un.org/press/en/2017/sc12714.doc.htm