**Country:** China

**Agenda Item:** Addressing the growing threat to Cybersecurity (UNSC)

**Introduction**

China is a densely populated major power in East Asia with advanced technology and is heavily reliant on electronic systems due to its role as a global manufacturer and its rapidly growing economy. China is vulnerable to cyber attacks as its reliance on electronic systems spans various crucial sectors including manufacturing, communication, transportation, finance, and defense.

**Topic and Country Relevance**

As countries are slowly converting their sectors and management into technological systems, cyber threats are getting more dangerous than ever before and are posing risks to governments. Some of the governments that are the most vulnerable to cyber-attacks are Iran, the US, Israel, Russia, India, NATO countries, and China as their nuclear facilities, communications, and army are managed by technological systems. In 2019, the UN passed a resolution named the “UN cybercrime treaty” which would criminalize cyber-attacks. The negotiations are still ongoing in 2024 but there isn’t much hope for the project as most states are not agreeing because of multiple reasons such as the treaty possibly criminalizing online free speech using loopholes as the conditions for taking action are broad and the rules are not yet clear. For these reasons, the project is considered a failure and there aren’t any other actions taken about the topic by the UN. Because of the mentioned reasons, the UN hasn't taken any international action about the growing threat to cybersecurity to this day.

**Solutions and Conclusion**

China’s Cyber Security Law (CSL) came into effect on 1st of June 2017. The CSL provides the CCP with the legal authority to inspect and investigate an organization for the safety of China’s intellectual property. It requires companies to store important and vulnerable data within China and allows Chinese authorities to conduct inspections and take action on a company's network. China’s CSL is also regulating the way critical data is stored, such as encryption of the specified data. All companies operating in China are required to obey the CSL. China’s laws about cybersecurity are driven mainly by national security and data protection, instead of the personal data of citizens. China expects the UN to take action on companies leaking governmental data and cyber-attacks on governmental systems, as well as the sabotage of nuclear power plants and nuclear centrifuges. China believes that cyber and internet traffic should be closely monitored by Chinese authorities and the UN to avoid negative impacts on China’s cybersecurity.

**References**

<https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter>

<https://news.un.org/en/interview/2024/02/1146772>

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

<https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law>