Committee: LEGAL
Agenda**:** International Regulations on Cybersecurity and Artificial Intelligence
Country: Republic of Korea
School: Keystone Schools

The Republic of Korea is a democratic nation in East Asia with a population of 52 million and its capital in Seoul. Despite our high quality of life, our education system remains highly competitive and stressful for students. Since our founding in 1948, Korea has grown into a major global economy with a GDP of 1.7 trillion dollars, relying heavily on exports such as semiconductors, vehicles, and ships. Our key partners include China, the United States, and Japan, and we maintain a strong military of about 500,000 active personnel.

The Republic of Korea recognizes that rapidly evolving technologies, especially AI, create both great opportunities and potential vulnerabilities. As one of the world's most digitally connected nations, the Republic of Korea has significant experience in cyber security. For which this level allows the Republic of Korea to be considered the safest online space in East Asia, receiving a score of 51 on the global safe internet space ranking. Such level of cyber security allowed the country to endure multiple online challenges targeting government buildings, finance centers and critical infrastructure, which in turn allowed it to strengthen its cyber security. Locally, the Republic of Korea has strengthened its legal structure through the Personal Information Protection Act (PIPA), national cybersecurity strategies, and the new AI Basic Act which is going to take effect in January 2026. Which promotes transparency, legal consequences, and human-dominated development of artificial intelligence. These policies shape Seoul's belief that international regulation must protect basic human rights, ensure safety, and defend national security while enabling the innovation necessary for long-term economic growth.

Internationally, the Republic of Korea supports a balanced, risk-based, and practical regulatory approach. Korea supports binding global movements against cybercrime, attacks on people's digital infrastructure, and irresponsible state behaviour online, while supporting adjustable international guidelines for AI jurisdiction that can evolve linearly with technology. Seoul pushes forward shared definitions of risky AI systems, minimum safety and transparency requirements and global teamwork on cybersecurity incident response. We as the Republic of Korea strongly believe that international law extends beyond real life and that states must collaborate to strengthen standards, information sharing, and capacity building—particularly with developing countries that face growing digital security gaps.

To conclude, the Republic Korea is dedicated to advancing international guidelines that safeguard human dignity, protect digital information, and promote responsible innovation. The Republic of Korea stands ready to lead through cooperation, share its technological advancements, and work toward a future where cybersecurity persistence and trustworthy AI, benefit all nations.
To finalise everything, the UN committee can advance cybersecurity and AI governance by establishing a realistic, cooperative International Cybersecurity and AI Safety Standard that sets a shared norm for protecting critical infrastructure, identifying high-risk AI, and ensuring

transparency and human oversight, reflecting South Korea's risk-based approach. Implementation should include a UN-managed capacity-building program, funded through optional contributions and collaborative partnerships, to provide training, technology transfer, and regular support for developing nations. Additionally, a global cyber response agency and information-sharing network should be created to manage real-time reporting, joint investigations, and quick assistance, ensuring practical, diplomatic, and globally beneficial protection of all digital ecosystems.

Sources:

1. https://asianintelligence.ai/south-korea
2. https://biz.chosun.com/en/en-it/2024/12/11/KOICFVLNBNFETMPJ5ONEKGQ6PI/
3. https://www.csis.org/analysis/ai-security-strategy-and-south-koreas-challenges
4. https://ps-engage.com/south-koreas-ai-framework-act-navigating-opportunities-and-challenges-before-enforcement/
5. https://babl.ai/south-korea-unveils-comprehensive-framework-for-ai-privacy-protection
6. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/