Committee: Legal
Country: Afghanistan
Delegate: ZEYNEP BEYZA AKAR
Agenda Item: International Regulations On Cybersecurity and Artificial Intelligence

Artificial intelligence and technology are increasingly being used in matters such as communicating with each other, security, and assisting the general public. While these features are awesome, they also pose some very severe threats to computer security. Countries like Afghanistan, which do not have very strong legislation, are easy targets for these threats.

The rapid advancement of Artificial Intelligence technologies and the growing complexity of cyber threats have created urgent legal and ethical challenges for the international community. As states increasingly rely on digital infrastructures for governance, security, and economic development, the risk of cyberattacks, data exploitation, and misuse of AI systems continues to expand. The Legal Committee plays a crucial role in developing frameworks that ensure the responsible use of AI and promote a stable, secure cyberspace. The delegation of Afghanistan firmly believes that effective international regulations must be grounded in state sovereignty, human rights, and equitable technological development.

In the United States and the UK, governments have formulated cybersecurity guidelines that should be adopted when developing and implementing AI systems. While not stringent laws, these guidelines affect how institutions and businesses apply AI systems effectively and safely. China has adopted a Cybersecurity Law, which promotes a strong focus on data protection control and critical information infrastructure. The law has specific restrictions on some AI use, particularly those associated with public information and security. This example illustrates the fusion between cybersecurity law and AI. If measures like these are not continued, it is absolutely undeniable that the misuse of artificial intelligence will increase.

In the context of Afghanistan, the following examples illustrate that complex systems are not necessarily needed from the onset by the Afghan government. Simple cybersecurity laws and the definition and limitations of use on high-risk AI systems could prove to be quite tangible initial steps forward by the government.

It should secondly set boundaries regarding the use of AI in major fields such as security and intercommunication. An AI system should aid human beings in a decision, and not make a decision on its own. There should be rules to avoid excessive espionage and unreasonable decisions made by the computer. In a nutshell Afghanistan should be able to come up with stronger computer safety regulations and AI policies by taking insights from other nations, incorporating ideas that work well. Computer threats, rights, and keeping Afghanistan stable for future generations are all achievable if laws are clear and easy to cooperate with. Technology is supposed to improve Afghanistan, not bring it complications that are beyond its control.

REFERENCES

1. https://economictimes.indiatimes.com/tech/technology/explained-what-the-ai-cybersecurity-guidelines-endorsed-by-the-us-uk-and-16-other-countries-entail/articleshow/105554278.cms?utm

2. https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China?utm

3. https://verifywise.ai/global-ai-regulations-and-frameworks-a-country-by-country-guide-for-legal-policy-and-grc-teams?utm

4. https://alia.org.tr/yapay-zeka-yasasi-avrupa-dijital-inovasyon-duzenlemesinde-bir-donum-noktasi?utm

5. https://sites.google.com/nist.ac.th/seasacmun2024/committees/disec?utm

6. https://cfecert.com/tr/yapay-zeka-hukukuna-kuresel-bakis/?utm

7. https://vodworks.com/blogs/ai-compliance/?utm

8. https://www.legalserviceindia.com/legal/article-17459-the-impact-of-artificial-intelligence-on-cyber-law.html?utm