

Committee: Disarmament and International Security

State: Democratic People's Republic of Korea

Agenda Item: Weaponization of Data and Cyber Security

Data armament and cyber security are necessary for the survival of a country. We have to understand that protection is an indispensable determinant for countries to upgrade living standards. As North Korea, in order to keep ourselves safe in cyberspace, we take many precautions and resort to organizational studies. For example, a 6.800-strong unit of trained cyber-warfare specialists are being operated and are working to enhance cyber capabilities by continuing R&D on the latest technologies. As information pollution in technological environments deeply affects societies, we, as a country, follow a closed and well-equipped path as required by our management style.

Furthermore, it should not be forgotten that misinformation and armament are not only dependent on the development of technology, it is a formation based on ancient times. It can be lived within a state as well as it can reach an international dimension. The event that occurs in this case between countries is information warfare. In this respect, races are held among many countries to gain competitive information advantage. We think that these races should be held in a controlled manner. The attacks carried out by the United States and South Korea deeply affected the DPRK. For this reason, our country, which is still in the recovery phase, organizes rigorous training for cyber defense and also for conflict actions. As of 2021, the measures taken against this problem and tactics related to the purpose of expanding the information network have begun to be arranged.

As the delegation of North Korea, we argue that the emergence of cyber crimes and problems such as information smuggling is unethical in some cases. Various attacks for emerging problems are carried out, and as a result, accurate data is damaged. Ethically, armaments cause tensions. Consequently, we should use artificial intelligence technologies to access more accurate information in order to eliminate information pollution and minimize problems. In this way, constriction between countries is reduced and data-based abuse of technology is prevented. To provide cyber security, countries should learn a number of things from each other and become better equipped for the methods used.

REFERENCES

https://keia.org/wp-content/uploads/2022/03/KEI_SMA_Harold-Mustafaga-Jun-Myers-Grossman

<https://www.cisa.gov/uscert/northkorea>

<file:///Users/ekinsmacbookair/Downloads/sustainability-14-01744.pdf>

<https://www.csis.org/programs/korea-chair/korea-chair-project-archive/north-koreas-cyber-capabilities>

<https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations>