Committee: Legal
Agenda Item: International Regulations on Cyber Security and Artificial Intelligence
Country: Turkiye
Delegate: ALI DENIZ DEMIREL

Introduction

Artificial Intelligence technology and the internet bring many new and good chances for all countries. They help us with trade, health and education. But they also bring big dangers. Cyberattacks are not just small problems they can hurt important services like hospitals, banks and electricity. Artificial Intelligence can also be used by bad actors to make stronger and faster attacks. This problem is important because it affects all countries and does not stop at borders. We need clear global rules for peace and safety.

Country's Background

The United Nations has already started working on this. The Open Ended Working Group is a place where many countries talk about making the internet safe. This group agrees that international law is important for the internet just like it is for other parts of the world. The United Nations Charter rules must be followed online. Organizations like the Global Partnership on Artificial Intelligence also help countries make sure Artificial Intelligence is used in a good and fair way that respects people's rights.

Country's Position

Türkiye believes that cyber security is a very important part of our national safety and economy. We have strong plans in our country, like the National Cyber Security Strategy and the National Artificial Intelligence Strategy. We use the Law on Protection of Personal Data to keep our citizens private information safe. Türkiye wants to work with other countries but we must protect our right to make our own rules about our internet space. The international rules must always respect the independence of our country.

Conclusion

Türkiye suggests the United Nations should take these simple and strong steps to make the internet safer:

1. We should make a special United Nations fund to help countries that need better security tools and expert training. This helps stop the whole world network from having weak spots.

2. We need to make simple, clear rules for how countries must act online. These rules must also look at the new dangers from Artificial Intelligence weapons and deepfakes.

3. All countries should make Computer Emergency Response Teams. We need a way to share information quickly about new attacks, so countries can protect themselves before the attack spreads.

References

1.Türkiye's National Artificial Intelligence Strategy Overview: https://www.oecd-events.org/smart-data-and-digital-technology-in-education/session/79d499e6-f200-ed11-b47a-a04a5e7cf9da/national-artificial-intelligence-strategy-2021-2025-turkiye

2. Türkiye's National Cybersecurity Strategy (2024-2028) Summary: https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2025%2Fdata%2FpolicyInitiatives%2F200001485

3. United Nations Open Ended Working Group on ICTs and Responsible State Behaviour: https://documents.un.org/doc/undoc/gen/n25/201/61/pdf/n2520161.pdf

4.Türkiye's Law on Protection of Personal Data summary: https://www.cookieyes.com/blog/turkey-data-protection-law-kvkk/

5. European Union Statement on the Role of Computer Security Incident Response Teams in United Nations Framework: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-united-nations-open-ended-working-group-ict-rules-norms-and-principals_en