Committee: DISEC

Country: Ukraine

Agenda Item: Weaponization of Data and Cyber Security

Cyberwarfare has played an important role in the Russo-Ukrainian conflicts since The Ouroborus tool kit began spreading into Ukrainian computer systems in 2010. Russia's cyber attacks continued with Operation Armageddon(2013), Operation Snake(2014), first(2015) and second(2016) power grid hacks, paralysis of the State Treasury(2016), NotPetya malware(2017) and the 2022 cyberattacks during the ongoing war.

Ukraine adopted a National Cybersecurity Strategy in 2016 that proposed update of the cybercrime legislation to meet the Budapest Convention requirements.The main focus of the Strategy is developing the national cybersecurity system, enhancing capabilities across the security and defence sector, and ensuring the cybersecurity of critical information infrastructure and of Government information resources. To address the needs taken up in the new Strategy, Ukraine has participated in a number of international cooperations including CyberCrime EaP II and CyberCrime EaP III (involving the Eastern Partnership) that aim to improve mutual legal assistance for the international cooperation on cybercrime and electronic evidence and to improve the cooperation between criminal justice authorities and service providers in specific criminal investigations and with the necessary rule of law safeguards. Ukraine is also working with the NATO Cyber Defence Trust Fund to enhance technical capabilities in counter cyber threats. Together with the NATO partners, The Security Service of Ukraine (taking the lead role in the framework of the Trust Fund) has conducted cyber defense exercises and trainings where all the relevant national stakeholders are trained on how react to major cyber attacks at the national defense infrastructure. Moreover, initiated by Ukraine, a working group on cybersecurity has been established in the framework of the GUAM Organization for Democracy and Economic Development.

Ukraine believes that ensuring cybersecurity nationwide and worldwide is on five axes:

- Developing a safe and sustainable cyberspace by improving legislation and establishing a steady system to identify and prevent cyber threats,
- Securing the electronic information resources by introducing new organizational and technical models of current cybersecurity systems and creating an integrated platform of safe electronic communications,
- Developing a critical infrastructure by improving regulations and developing public-private partnerships,
- Developing the cybersecurity capacity by improving the training programmes for personnel and establishing cybersecurity components across defence forces,
- Preventing cybercrime by establishing contact centers for reporting crimes in the cyberspace, training law enforcement personnel to handle digital evidence and improve procedural tools for digital forensics.

Resources:

- https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/
- https://en.wikipedia.org/wiki/Russian%E2%80%93Ukrainian_cyberwarfare
- https://www.ft.com/content/20544951-2c98-4d47-842d-b34a246a564f
- https://www.coe.int/en/web/cybercrime/cybercrime-eap-iii
- https://www.coe.int/en/web/cybercrime/cybercrime-eap-ii