SESSION 13

Cybersecurity and Resilience – Connecting the Regulatory and Technical Agendas

Suzi Szeredi, Programme Director, Transatlantic Policy Network

- Parliamentarians presented the recently agreed (as well as proposed) legislation to be adopted by the EU during this mandate. Panelists reaffirmed the timeliness of these cybersecurity proposals. A key issue under discussion includes the skills element so key to delivery behind the new proposals, which the Cybersecurity Skills Academy is designed to address.

- While some cyber incidents come from hacking, many are derived from simple human errors. As innovation happens at the company level, it is ever more important to leverage private sector expertise by building operational public-private partnerships and cooperating upstream at the technological innovation stage. This approach was recently endorsed in the statement by Presidents Biden and Von der Leyen.

- With the increasing digitalization of public services, the threats 'surface' is increasing, and so is the need for cybersecurity. Estonia is a good case study where a Centre for Excellence now operates. Ukraine is digitalizing at a rapid pace. This debate will be ever more important with the upcoming elections next year.

- While legislating cyber is not necessarily political, the means to do it are. Governments either have to hire state-of-the-art expertise or rely on outsourcing to the private sector. In all cases, cybersecurity skills and education will be essential.

- As the telecom sector set out its experience in security over the past century, underlining the investment required to maintain trust, the challenge for SMEs was emphasized. For most SMEs, the resources available to big corporates are not available, and cybersecurity remains an existential threat to their business. Hence, the focus in Europe is on cyber solidarity and a protective architecture that is available to SMEs.

- The challenge of legislating cyberspace is real, especially in the cyber-defense dimension. Many Member States are reluctant to share data or only with given countries. Flexibility should be allowed while understanding that dividing cyberspace into an internal and external dimensions is not feasible as it is inherently cross-border and cross-sectoral. Indeed, threats may originate not only from private sector driven financial gains but also from public actors such as third-country governments.

- The legislative difficulty and the multi-stakeholder environment raise questions as to whether current arrangements for transatlantic cooperation are adequate. As they currently take place under the aegis of NATO, the EU-US Cyber Dialogue. and within dedicated private sector fora, the idea of creating a Working Group under the Trade and Technology Council was raised and supported provided that the private sector is included.