Cyber Conflicts & Critical Infrastructure: What Happens When Systems Fail?

Cyberattacks have become a major instrument in contemporary security and conflict. Critical infrastructure, including energy grids, transportation networks, hospitals, and financial systems, is increasingly targeted, creating risks of wide-ranging disruption. State and non-state actors, including sophisticated cyber units from Russia, China, and other countries, exploit vulnerabilities for strategic, economic, or political purposes. This working group examines the types of threats facing critical systems, the consequences of large-scale disruptions, and the strategies and policies that can enhance resilience, preparedness, and response in the cyber domain.

Summary of the Discussion in the Working Group

The working group discussions were highly dynamic and interdisciplinary, bringing together participants from international relations, law, computer science, and software engineering. This diversity gave the group a great opportunity for a comprehensive understanding of cybersecurity challenges from technical, legal, and geopolitical perspectives. This had a huge impact on scope and deeper understanding of the issue, enabling not just to share the group's pre-existing knowledge but to learn.

Over the two days, the group focused on the protection of critical infrastructure in the context of hybrid warfare. Experts included a military specialist who discussed emerging military technologies and hybrid threats, and a representative from a cybersecurity agency in The Hague, who explained the theoretical foundations, technical aspects and evolution of cybersecurity. Both sessions had incredibly active engagement, allowing participants to ask questions, allowing them to deepen our understanding.

Key Questions Emerging from the Discussion

- When does the cyber attack cross the threshold of an use of force and is there a need to change the legal framework in order to better respond to non-armed attacks?
- How can we make sure that a just and efficient government remain democratically legitimate? What role could Ai play in that?

Summary of the Discussion at the Closing Panel

During the Closing Event of the Young European Security Conference 2026, the discussion focused on the resilience of critical infrastructure in the context of evolving cyber threats, including but not limited to Russia's war against Ukraine and other case studies. The group presented their key findings and policy recommendations, emphasizing the need for stronger EU-level coordination, public-private cooperation, and emphasised on the current necessity of cyber resilience.

Panelists actively engaged with the proposals, reflecting on both practical challenges and long-term strategies. In response, the group's representative posed questions regarding the implementation gap between policy frameworks and real-time crisis response. One of the speakers noted that "resilience is no longer optional, but a core element of national security." The discussion highlighted the urgency of translating policy into actionable mechanisms capable of responding to hybrid threats.