Published: 25.03.2026

# Second meeting of the BSPC Working Group on Strengthening Cyber and Information Resilience

On 22-23 March 2026, the parliamentarians of the Baltic Sea states met in the second meeting of the Baltic Sea Parliamentary Conference (BSPC) Working Group on Strengthening Cyber and Information Resilience to Promote Democracy (WG SCIRPD) in Szczecin, Poland.

Chair of the WG SCIRPD and Member of the Security and Defence Committee of the Baltic Assembly Meelis Kiili opened the meeting by emphasising that, since the inaugural session in Tallinn, the threat landscape has continued to evolve. Russian hybrid operations across the region have grown increasingly sophisticated. At the same time, the EU's regulatory agenda on cybersecurity and AI is accelerating, with instruments such as the NIS2 Directive, the Cyber Resilience Act and the AI Act requiring national implementation. "Cyber threats and disinformation campaigns do not only endanger technological systems - they undermine trust, stability and security across the region," he stated.

## Expert presentations

President of the Institute of Socio-Political Technologies "Kybernetes" and leader of the Scientific Team of the Advisory Council for Resistance to International Disinformation at the Ministry of Foreign Affairs of Poland Mariusz Żabiński presented a model for developing new value-congruent capabilities for resilience and addressing Foreign Information Manipulation and Interference (FIMI) - Resilience Councils and the Teleo-Systemic Approach. He noted that countering FIMI and strengthening resilience requires accelerated regulatory action and the development of advanced technological tools. It also calls for stronger cross-sectoral cooperation across government, industry, academia and the civil society as a whole. At the same time, engaging the younger

generation as active partners is essential, while long-term success will depend on enhancing technological sovereignty and strengthening analytical capabilities.

Dominika Skoczylas from the Faculty of Law and Administration at the University of Szczecin highlighted the role of cybersecurity policies as a tool to support the protection of democracy and the development of the information society. She emphasised that cybersecurity policies should address the security of electronic services across both the public and private sectors, as well as critical infrastructure and users within the information society. She also noted the importance of skills to deal with incidents or introduction to long-term solutions and establishment of relevant institutions, alongside strengthened international cooperation.

External Threat Analysis Expert at the Cyberspace Information Protection Division of NASK Filip Głowacz informed about Russian hybrid threats or a mix of tools below open war, such as economic pressure, military probes, sabotage, cyber, information and psychological operations against Poland. The presentation also highlighted the role of media in the context of hybrid threats, noting that the unintentional amplification of harmful narratives can contribute to the spread of disinformation. He stressed the importance of closer cooperation between media, NGOs and governments, as well as the need for greater awareness and education among journalists on the nature and impact of the information they disseminate.

Attorney-at-law and ISO 27001/22301 Lead Auditor, Law & Patent Office MALUJDA.PL Rafał Malujda highlighted cyber crisis management as a central pillar of cyber resilience and an essential element in safeguarding democratic systems. He emphasised that preparedness for high-impact cyber incidents requires not only technical capabilities but also well-developed coordination and decision-making processes. In this context, tools such as tabletop exercises and simulation-based training are particularly valuable, as they allow stakeholders to test responses in realistic stress scenarios and generate practical lessons learned. In addition, the importance of a coherent regulatory framework was underscored, particularly

regarding legal clarity on sensitive issues such as the payment of ransom in the event of ransomware attacks.

During the meeting, members of the WG SCIRPD reviewed the recommendations put forward following the inaugural meeting in Tallinn, proposed additional topics for inclusion in the report and future discussions, and considered plans for upcoming meetings.

## Visit to the Autocomp Management

The members of the WG SCIRPD also had the opportunity to visit Autocomp Management, an international manufacturer and supplier of technologically advanced systems supporting training for the national defence sector and uniformed services of Poland, as well as for rail, road and water transport. Research and Development Director Roman Haberek shared insights into their work. Solutions offered by Autocomp Management are open systems that can be delivered as standalone modules, subsystems for third-party training platforms, as well as allowing the addition of third-party training simulator modules. Their largest foreign partner is the German Krauss Maffei Wegmann company, for which they provide tank simulators Leopard 2A4/2A5 and a whole group of vehicles based on the Leopard chassis. Since 2019, Autocomp Management has been included in the list of entrepreneurs of special economic and defence importance.

Pomorze
Zachodnie
Pomorze
Zachodnie