**Annual OSCE-wide Chairpersonship Conference on Cyber/ICT Security**

***Resilient Cyberspace: Principles, Partnerships, and the Path Ahead***

**Date: 30 September - 2 October 2025**

**Venue: Radisson Blu Seaside Hotel, Helsinki**

## Concept Note

Accelerating digitalization, development of new technologies and continually growing interdependencies are altering the global operating environment. Threats have become increasingly diverse and cyber is becoming the key domain and means for hybrid influencing activities, crime, terrorism and warfare.

While states bear primary responsibility for the maintenance of international peace and security, numerous other stakeholders such as the private sector, civil society and academia are critical for promoting stability and advancing responsible behaviour in cyberspace.

The OSCE has a clear and important role in cyber security. The Organization's sixteen voluntary Confidence Building Measures (CBMs) have the potential to reduce tensions and enhance security in cyberspace. These measures have inspired the wider global community to adopt similar ones. This shows how the OSCE can be innovative, adapt to changing circumstances and test new ideas. Finland advocates for an open, free, secure and stable cyber domain where the rule of law, responsible state behaviour, democracy and human rights are respected. There is a clear need to advance the concrete implementation of international rules, norms and principles as well as responsible state behaviour in cyberspace.

The Annual Chairpersonship Conferences on Cyber/ICT Security are an excellent means of exploring cyber security in the OSCE region. The conference in Helsinki will be an opportunity to continue the discussions of the previous Chairpersonship Conference on "Strengthening

National Cyber Resilience", organised in Malta, as well as the meetings of the Informal Working Group Established by PC Decision 1039 and related side events.

The first session of this year's conference offers an insightful keynote address setting the stage for the discussions ahead. Related to the Finnish Chairpersonship priority of respecting the commonly agreed principles and enhancing multilateral cooperation, the second session explores responsible state behaviour in cyberspace. As the OSCE cyber/ICT security CBMs are widely seen as state-of-the-art, the session will also look at what can be learned from their implementation as a way to advance responsible state behaviour.

The third session builds on the side event "Public-Private Partnerships and the Whole-of-Society Approach to Cyber Security" organised by Finland on 10 March and highlights the role of public-private partnerships in responding to cyber security threats and enhancing cyber resilience. The final session prepares for the future. It explores how to respond to the challenges posed by artificial intelligence and disruptive technologies, but also their potential to have a positive impact on peace and security, and what kind of policies and actions are needed to seize that potential.

The conference will bring together high-level officials from the OSCE, the participating States and Partners for Co-operation, as well as representatives of civil society, academia and the private sector, and other international organisations.

A meeting of the Informal Working Group Established by PC Decision 1039 and an informal gathering on Uunisaari island will precede the conference on Tuesday, 30 September. The conference will open on Wednesday, 1 October at 09.00 and run until 17.30, followed by a reception. On Thursday, 2 October, a series of side events and excursions will be offered, showcasing different aspects of public-private partnerships at cyber/ICT related organisations - such as the Technical University, a private company and internal security authorities. Further information and registration links for the side events and excursions will be shared in September.

# DRAFT Agenda

## Tuesday, 30 September

09:00-11:00 Registration

11:00-17:00 **Meeting of the Informal Working Group Established by PC Decision 1039**

(separate agenda and registration)

18:00 **Informal get-together on Uunisaari island**

## Wednesday, 1 October

08:00-09:00 Registration

09:00-09:30 **Opening of the OSCE-wide Chairpersonship Conference on Cyber/ICT Security**

- Ambassador Jukka Salovaara, Permanent State Secretary at the Ministry for Foreign Affairs of Finland
- Ambassador Alena Kupchyna, OSCE Coordinator of Activities to Address Transnational Threats

09:30-10:15 **Session 1: Setting the scene**

The first session will set the stage for the discussions ahead with an insightful keynote address by Mr Mikko Hyppönen, Chief Research Officer of Sensofusion. The session includes a possibility for Q & A.

10:15-10:45 Coffee break

10:45-12:30 **Session 2: Respecting the principles: How to advance responsible state behaviour in cyberspace, including through CBMs**

As the 2025 OSCE Chair, Finland prioritises respect for the commonly agreed principles. In line with this, the second session explores responsible state behaviour in cyberspace. Furthermore, the session will look at what can be learned from the implementation of the OSCE cyber/ICT security CBMs as a way to advance responsible state behaviour.

The panel discussion is moderated by Ambassador Marek Szczygieł, Permanent Representative of Poland to the OSCE and Chair of the Informal Working Group Established by PC Decision 1039. The panellists are:

- Dr Annegret Bendiek, European Repository of Cyber Incidents

- Mr Felix Kroll, Head of Cyber Foreign Policy and Cyber Security Coordination Staff, Federal Foreign Office of Germany
- Dr Patryk Pawlak, Part-Time Professor, Robert Schuman Centre and Project Director, Global Initiative on the Future of the Internet (GIFI)
- Ms Yrysty Zhalilkhanova, Committee for Information Security of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan

Guiding questions for the session:

- What can be done to further enhance responsible state behaviour in cyberspace?
- What is the OSCE's added value in cyber security and cyber diplomacy?
- How can the OSCE best support states in translating abstract international obligations into actionable national policies, legal frameworks, and institutional practices?
- How to use the cyber/ICT security CBMs to strengthen cooperation between states?
- How do asymmetries between cyber-capable and less-capable states affect the credibility and uptake of CBMs?
- How can civil society and the private sector contribute to the development and implementation of cyber CBMs?

12:30-13:30 Lunch break

13:30-15:30 **Session 3: Responding today: The role of the whole-of-society approach and private sector in addressing cyber security threats**

The third session highlights the role of public-private partnerships in responding to cyber security threats and enhancing cyber resilience. The session starts with a keynote address by Mr Anton Demokhin, Deputy Foreign Minister and Chief Digital Transformation Officer of Ukraine.

The keynote address is followed by a panel discussion moderated by Ms Szilvia Tóth, Cyber Security Officer at the OSCE Secretariat. The panellists are:

- Ms Sanja Catibovic, National Project Officer, OSCE Mission to Bosnia and Herzegovina
- Mr Stelian Cristea, Deputy Director, Romanian National Cyber Security Directorate
- Ambassador Helen Popp, Ambassador at Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia
- Ms Tinna Sigurdardottir, Senior Analyst, European Centre of Excellence for Countering Hybrid Threats

- Mr Peter Sund, CEO, Finnish Information Security Cluster

Guiding questions for the session:

- How do the roles of the public authorities, private sector and civil society, including research community, differ in building cyber resilience and cyber security?
- What incentives and frameworks can help ensure sustained private sector engagement in national and regional cyber resilience efforts?
- How can trust be built between stakeholders with differing priorities, especially in crisis response scenarios?
- Cybersecurity can be framed narrowly as a technical issue, rather than a societal one. How can we broaden the narrative?
- What role does digital literacy and public awareness play in building societal cyber resilience?

15:30-16:00 Coffee break

16:00-17:15 **Session 4: Preparing for the future: Seizing opportunities and responding to the challenges posed by AI and disruptive technologies**

The final session explores how to respond to the challenges posed by artificial intelligence (AI) and disruptive technologies, but also their potential to have a positive impact on peace and security.

The panel discussion is moderated by Ms Johanna Poutanen, Head, Inclusion & Digital Innovation at CMI – Martti Ahtisaari Peace Foundation. The panellists are:

- Dr Samuele Dominioni, Cybersecurity Researcher, United Nations Institute for Disarmament Research (UNIDIR)
- Mr Stefan Lee, Cyber Ambassador, Ministry for Foreign Affairs of Finland
- Mr Philippe Tremblay, Director of the Office of the OSCE Representative on the Freedom of the Media
- Mr Johan Turell, Head of the Office for Strategic Cybersecurity, Swedish Civil Contingencies Agency
- Dr Juha Vartiainen, Co-founder and Chief Global Affairs Officer, IQM Quantum Computers

Guiding questions for the session:

- What policy choices are needed to seize the positive potential for peace and stability while mitigating the risks posed by AI and disruptive technologies?
- What kind of a role should the OSCE and other multilaterals have in making these policy choices?
- How to have an inclusive dialogue on AI and disruptive technologies?

- What lessons can be drawn from past technological disruptions (e.g. the internet, social media) to guide our response to AI?
- What OSCE capacity-building efforts are needed to help participating States develop resilient, rights-respecting AI governance frameworks?
- AI and disruptive technologies cut across the OSCE's three dimensions. How can the Organization develop an efficient and coherent approach that enhances complementarity across them?

17:15-17:30 **Conference Closing**

- Mr Heikki Tamminen, State Secretary at the Ministry of the Interior of Finland

17:30-19:00 Reception

- Welcome words by Ambassador Jouni Laaksonen, Head of the Task Force for the Finnish OSCE Chairpersonship

## Thursday, 2 October

09:30-12:00 **Parallel side events and excursions (registration beforehand)**

09:30-11:30 Side-event "Operationalizing Cyber Security: Internal Security and the Finnish Comprehensive Model"
Hotel Radisson Blu Seaside, meeting room Nobel (3rd floor)

10:00-11:30 Visit to Nokia Executive Experience Center
Bus transportation from Hotel Radisson Blu Seaside at 09:30
Return to hotel by 12:00

10:00-11:30 Visit to Aalto University and the Cyber Citizen Project
Bus transportation from Hotel Radisson Blu Seaside at 09:30
Return to hotel by 12:00

10:00-11:30 Visit to Museum of Malware Art
Bus transportation from Hotel Radisson Blu Seaside at 09:45
Return to hotel by 12:00